现代数学基础

13

数论 II

——岩泽理论和自守形式

■ 黑川信重　栗原将人　斎藤毅　著

■ 印林生　胥鸣伟　译

高等教育出版社
HIGHER EDUCATION PRESS

academic.hep.com.cn

定价 29.00 元

■ 学科类别：数学

现代数学基础

13 数论 II

—— 岩泽理论和自守形式

高等教育出版社
HIGHER EDUCATION PRESS

图字：01–2009–1458 号

数論 II —— 岩澤理論と保型形式
黒川信重，栗原将人，斎藤毅

SURON, II: IWASAWA RIRON TO HOKEI KEISIKI
by Nobushige Kurokawa, Masato Kurihara, and Takeshi Saito

Originally published in Japanese by Iwanami Shoten, Publishers, Tokyo, 2005.
This simplified Chinese language edition published in 2009
by the Higher Education Press, Beijing
by arrangement with the proprietor c/o Iwanami Shoten, Publishers, Tokyo

图书在版编目（CIP）数据

数论.2,岩泽理论和自守形式/(日)黑川信重,(日)栗原将人,(日)斎藤毅著；印林生，胥鸣伟译.—北京：高等教育出版社,2009.6

ISBN 978-7-04-026361-9

Ⅰ.数… Ⅱ.①黑…②栗…③斎…④印…⑤胥… Ⅲ.数论 Ⅳ.O156

中国版本图书馆 CIP 数据核字（2009）第 042794 号

策划编辑 赵天夫　**责任编辑** 李　鹏　**封面设计** 张　楠　**责任绘图** 尹文军
版式设计 余　杨　**责任校对** 杨凤玲　**责任印制** 朱学忠

出版发行	高等教育出版社	购书热线	010－58581118
社　　址	北京市西城区德外大街 4 号	免费咨询	400－810－0598
邮政编码	100120	网　　址	http://www.hep.edu.cn
总　　机	010－58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京新丰印刷厂	畅想教育	http://www.widedu.com
开　　本	787×1092　1/16	版　　次	2009 年 6 月第 1 版
印　　张	13.25	印　　次	2009 年 6 月第 1 次印刷
字　　数	280 000	定　　价	29.00 元

物料号　26361–00

内容提要

本书在《数论 I》的基础上，进一步迈向现代数论的两大主题：解析方面的自守形式和代数方面的岩泽理论，以及二者之间的联系。在自守形式方面介绍了模形式、Eisenstein 级数、自守形式与表示论之间的关系以及 Langlands 猜想等。在岩泽理论方面介绍了分圆 $\mathbb{Z}_p$ 扩张、p 进 ζ 函数、岩泽主猜想及与自守形式的关系等。最后不予证明地介绍了 Wiles 对 Fermat 大定理的证明。这是读完本书后可进一步学习的主要方向之一。

本书适合于数论和相关专业研究生的学习，也可以作为数论研究工作者的参考书。

中文版序言

我们非常高兴看到我们的日文著作《数论》的中文版。我们十分感谢译者、编辑和出版者。

希望本书的中译本能吸引更多的中国读者探索数的奥妙，并进一步促进日中的学术交流。

全体作者代表
斋藤毅
2009 年 4 月

前　　言

数论魅力的源泉在于素数所具有的奇特性质。为了要弄清素数, 研究数论的人们开发出了各式各样的手段和方法。对于 ζ 函数以及类域论, 我们已在《数论 I》中见到过了。本书是《数论 I》的延续, 对于构成现代数论基础的重要理论进行了阐述。现代数论的特征可以说成是, 它的代数的方面与它的解析的方面相互缠绕在一起。所谓的代数方面是指数域、Galois 群还有代数几何的对象之类的, 而解析方面则是指 ζ 函数、自守形式还有自守表示之类的。譬如, 由高木贞治所完成的类域论的核心部分表现为 Galois 群的一维表示这个代数对象与伊代尔类群的一维表示 (Hecke 特征) 这个解析对象具有同一个 ζ 函数。因此在本书所处理的岩泽理论中, 作为 ζ 函数的 p 进化身的 p 进 L 函数是作为解析对象出现的, 它的代数的、数论的意义正在被弄清。

以将类域论推广到非交换 Galois 群的情形作为目标并正在建设之中的 "非交换类域论", 是现代数论的一个巨大的主题。其最初的例子是, 有理数域上的椭圆曲线这个代数对象, 与相关于模群的同余子群的自守形式这个解析对象之间的对应。根据所确立的这个对应, Wiles 解决了自问题提出已有 375 年之久的 Fermat 猜想的证明。这个伟大事件发生距今恰好 10 年了。

本书以这样的现代数论的动向为背景介绍了自守形式和岩泽理论的基础理论, 另外还以对 Wiles 的 Fermat 猜想的证明概述为中心介绍了椭圆函数的算术。每章都借助于具体的计算以增进理解。无论如何, 希望读者能动手来体验一下现代数论。还要说一句, 这本书曾作为岩波讲座的现代数学基础发行的《数论 3》的单行本出版过。

黑川信重, 栗原将人, 斋藤毅
2004 年 11 月 11 日

理论的概要与目标

本书是在《数论 I》(原来的 1,2) 的基础之上, 迈步走向了现代数论的两个代表性的主题。所说的两个主题就是在解析方面的自守形式论和在代数方面的岩泽理论。

自守形式分为第九章和第十一章。第九章以 Ramanujan 所发现的几个漂亮的等式的证明为目标, 考察了相对于模群的自守形式。特别地, 研究了 Eisenstein 级数与尖点形式。另外还引进了在现代数论中常常用到的 ζ 正规化积, 并证明了 Kronecker 极限公式。在这里本质性的内容是自守性。如其名字所示, 自守形式的要点是自守性. 所谓自守性就是满足某种形式的函数方程, 由于这是个特别强的条件, 故自守形式要依据具体情况而决定。其结果是使用自守性以及 Kronecker 极限公式, 就得到了 Ramanujan 的等式。在第十一章中, 为了从更广的观点眺望自守形式, 我们对群上的自守形式以及 Selberg 迹公式进行了展望。

第十章处理了岩泽理论。我们尽可能以容易理解的方式以岩泽主猜想为中心讲解了经典的岩泽理论。ζ 函数在整数的值中间有着 p 进的联系, 而这个现象由于 p 进 L 函数的存在变得可以得到清楚的理解。我们先对 p 进 L 函数进行讲解 (§10.1), 而后则叙述了所谓的岩泽 $\mathbb{Z}_p$ 扩张理论 (§10.2)。在这里, 我们研究了数论中的重要研究对象理想类群, 包括 Galois 群的作用, 特别地以 $\mathbb{Z}_p$ 扩域上的理想类群 (按照类域论, 这也可以说是最大非分歧 Abel 扩域的 Galois 群) 作为研究的目标。而且, §10.1 与 §10.2 的结果按照岩泽主猜想被联结了起来 (§10.3)。第十二章中, 在花了不少篇幅讲解了有关椭圆曲线的算术的基本事实后, 我们便来到了 Wiles 所给出的 Fermat 猜想证明的路线上了, 从而简洁地讲解了他的证明思想。

通过本书, 希望读者能品味到现代数论的乐趣。更希望能将本书作为基础深入钻研, 从而进入到数论研究的第一线。

目　　录

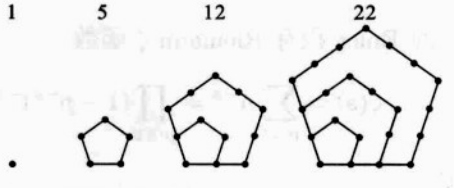
数论 I 的内容

第九章　何谓自守形式

自守形式最早出现在 1750 年 Euler 的五角数定理中:

$$\prod_{n=1}^{\infty}(1-q^n)=\sum_{m=-\infty}^{\infty}(-1)^m q^{\frac{3m^2-m}{2}}.$$

这里右端出现的 $\dfrac{3m^2-m}{2}=1,5,12,\cdots$ 为 5 角数 (《数论 I》§0.5).



称 Euler 等式的左端为 η 函数, 右端为 ϑ 函数, 这些便是 Euler 给出的自守形式的原型. 在其后的 1859 年, Riemann 研究了自守形式 ϑ, 它出现在 $\zeta(s)$ 的积分表示 (第七章) 中, 从而迎来了自守形式的 ζ 研究的新局面. 按照 Riemann 的积分表示, ϑ 的自守性转移到了 $\zeta(s)$ 的函数方程上.

在这种背景之下, 是 Ramanujan 发现了作为现代自守形式理论基础的新型的 ζ (1916 年). Ramanujan 研究了函数

$$\Delta(z)=q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

的 Fourier 展开

$$\Delta(z)=\sum_{n=1}^{\infty}\tau(n)q^n$$

中出现的系数 $\tau(n)$. 在这里 $q=e^{2\pi iz}$, 其中 z 为**上半平面** (upper half plane)

$$H=\{z\in\mathbb{C}\mid \mathrm{Im}(z)>0\}$$

中的变量. 因此 q 的绝对值小于 1, 从而 $\Delta(z)$ 的无限积表示和它的 Fourier 展开都绝对收敛. 这个 $\Delta(z)$ 在自守形式中显得尤其漂亮.

自守形式 (automorphic form) 的名字意味着 " 保持形式不变", 在 $\Delta(z)$ 的情形, 这种自守性表示为

$$\Delta\left(\frac{az+b}{cz+d}\right)=(cz+d)^{12}\Delta(z)$$

对于所有

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$$

(就是说, $a,b,c,d\in\mathbb{Z}$ 且满足 $ad-bc=1$) 成立. 称 $(cz+d)^{12}$ 里的 12 为**权** (weight), 因此说 $\Delta(z)$ 是权为 12 的自守形式.

Ramanujan 发现的新型 ζ 是

$$L(s,\Delta)=\sum_{n=1}^{\infty}\tau(n)n^{-s},$$

并猜测 $L(s,\Delta)$ 具有 Euler 积表示

$$L(s,\Delta)=\prod_{p:\text{素数}}(1-\tau(p)p^{-s}+p^{11-2s})^{-1}.$$

到这里为止我们见到的 Euler 积有 Riemann ζ 函数

$$\zeta(s)=\sum_{n=1}n^{-s}=\prod_{p:\text{素数}}(1-p^{-s})^{-1}$$

以及 Dirichlet L 函数

$$L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}=\prod_{p:\text{素数}}(1-\chi(p)p^{-s})^{-1},$$

它们的每个局部因子都仅仅是 p^{-s} 的一次式 (这是本质性的). Ramanujan 发现了 2 次的 Euler 积, 同时提出了猜想, 即被称做 **Ramanujan 猜想** (Ramanujan conjecture) 的

$$|\tau(p)|<2p^{\frac{11}{2}}$$

(这等价于在 Euler 积中出现的二次式的判别式为负). 这给出了 20 世纪数论发展的一个原动力. 而且, 具有这样的 2 次 Euler 积的 ζ 终究是成就 Fermat 大定理解决的关键, 它的解决是与装点 20 世纪闭幕仪式相匹配的令人惊喜的事件, 这是 Ramanujan 肯定没有想到的.

现代数论进一步地把目标指向更高次 Euler 积的研究. 在这一章中我们一方面追寻 Ramanujan 所发现事实的证明, 另一方面则要进行具体的处理, 并要引进自守形式.

那么, 自守形式理论的特点是由自守性这一强的条件可以推导出非常多的不只是像猜想中那样的等式. 这大概是它特别吸引 Ramanujan 的理由吧. 在这一章中, 我们应用自守形式证明, 譬如, 下面这样的等式:

$$\sum_{n=1}^{\infty} \frac{n^5}{e^{2\pi n}-1} = \frac{1}{504}$$

$$\sum_{n=1}^{\infty} \frac{n}{e^{2\pi n}-1} = \frac{1}{24} - \frac{1}{8\pi}$$

$$\sum_{n=1}^{\infty} \frac{n^3}{e^{2\pi n}-1} = \frac{1}{80}\left(\frac{\varpi}{\pi}\right)^4 - \frac{1}{240}$$

$$\sum_{n=1}^{\infty} \frac{1}{n(e^{2\pi n}-1)} = -\frac{\pi}{12} - \frac{1}{2}\log\left(\frac{\varpi}{\sqrt{2\pi}}\right).$$

这里, π 是通常的圆周率

$$\pi = 2\int_0^1 \frac{dx}{\sqrt{1-x^2}} = 3.14159\cdots,$$

而

$$\varpi = 2\int_0^1 \frac{dx}{\sqrt{1-x^4}} = \frac{\Gamma\left(\frac{1}{4}\right)^2}{2^{\frac{3}{2}}\pi^{\frac{1}{2}}} = 2.62205\cdots$$

则是距今 (2004 年) 正好 200 年前 Gauss 所考虑的与圆周率类似的叫做 "双纽线 (lemniscate) 周率" 的数. 由于这些等式的难度在缓慢地加深, 希望读者能边读边品味.

§9.1 Ramanujan 的发现

1916 年 Ramanujan 对于在

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \quad (q = e^{2\pi iz})$$

的 Fourier 展开

$$\Delta(z) = \sum_{n=1}^{\infty}\tau(n)q^n$$

中出现的系数 $\tau(n)$ 进行了大量的计算:

$$\begin{array}{llll} \tau(1)=1, & \tau(2)=-24, & \tau(3)=252, & \tau(4)=-1472, \\ \tau(5)=4830, & \tau(6)=-6048, & \tau(7)=-16744, & \\ \tau(8)=84480, & \tau(9)=-113643, & \tau(10)=-115920, & \cdots. \end{array}$$

凝视着这些得到的数, Ramanujan 提出了下面的猜想 ①, ②, 并进行了 ③ 的证明:

① 令 $L(s,\Delta)=\sum_{n=1}^{\infty}\tau(n)n^{-s}$, 则 $L(s,\Delta)=\prod_{p:\text{素数}}(1-\tau(p)p^{-s}+p^{11-2s})^{-1}$.

② 对于素数 p 有 $|\tau(p)|<2p^{\frac{11}{2}}$.

③ 对于素数 p 有 $\tau(p)\equiv 1+p^{11} \mod 691$.

它们之中的 ① 在次年即 1917 年由 Mordell 利用算子 $T(p)$ 予以证明. ② 则在近 60 年后的 1974 年由 Deligne 利用代数几何的手段予以证明. 猜想 ②(单称为 Ramanujan 猜想) 被归结到了作为 Riemann 猜想的代数几何类比的 Weil 猜想, 而 ③ 则给出了思考 l 进表示的一个启示 (691 是个素数). Deligne 的方法是以 Grothendieck 对代数几何的创新为基础的, 对此, 现代数学进展的岩波讲座“Weil 猜想与 Etale 上同调” 有所叙述.

本节要进行对 ① 与 ③ 的证明. 但是, 为此利用 $\Delta(z)$ 的作为自守形式的性质是必需的, 为了使证明的推理易于理解, 这些事实将放在 §9.2 给予证明.

(a) Mordell 的证明

现在来证明 Ramanujan 猜想, 而 Mordell 给出了证明的结果.

定理 9.1 (Mordell, 1917 年)

$$\sum_{n=1}^{\infty}\tau(n)n^{-s}=\prod_{p:\text{素数}}(1-\tau(p)p^{-s}+p^{11-2s})^{-1}.$$

[证明]　Mordell 对于每个素数 p 构造了 **Mordell 算子**(Mordell operator)

$$(T(p)\Delta)(z)=\frac{1}{p}\sum_{l=0}^{p-1}\Delta\left(\frac{z+l}{p}\right)+p^{11}\Delta(pz). \tag{9.1}$$

并证明了

$$T(p)\Delta=\tau(p)\Delta$$

(即 Δ 为 $T(p)$ 的特征函数而 $\tau(p)$ 为其特征值). 我们首先来看由此等式如何得到定理 9.1(Ramanujan 的 ①). 现将

$$\Delta(z)=\sum_{n=1}^{\infty}\tau(n)q^n$$

代入 $(T(p)\Delta)(z)$ 的表达式中, 于是

$$(T(p)\Delta)(z) = \frac{1}{p}\sum_{l=0}^{p-1}\sum_{n=1}^{\infty}\tau(n)\exp\left(2\pi in\frac{z+l}{p}\right) + p^{11}\sum_{n=1}^{\infty}\tau(n)q^{pn}$$

$$= \sum_{n=1}^{\infty}\left(\frac{1}{p}\sum_{l=0}^{p-1}e^{2\pi in\frac{l}{p}}\right)\tau(n)q^{\frac{n}{p}} + p^{11}\sum_{n=1}^{\infty}\tau(n)q^{pn},$$

其中

$$\frac{1}{p}\sum_{l=0}^{p-1}e^{2\pi in\frac{l}{p}} = \begin{cases}1 & p|n\\ 0 & p\nmid n.\end{cases}$$

因此有

$$(T(p)\Delta)(z) = \sum_{n=1}^{\infty}\tau(pn)q^n + p^{11}\sum_{n=1}^{\infty}\tau(n)q^{pn} \tag{9.2}$$

$$= \sum_{n=1}^{\infty}\left(\tau(pn) + p^{11}\tau\left(\frac{n}{p}\right)\right)q^n.$$

但是, 一般地如果 $x \notin \mathbb{Z}$ 则令 $\tau(x) = 0$. 特别地当 $p \nmid n$ 时有 $\tau\left(\frac{n}{p}\right) = 0$.

因此应用 $T(p)\Delta = \tau(p)\Delta$ 便得到了

$$\tau(pn) + p^{11}\tau\left(\frac{n}{p}\right) = \tau(p)\tau(n) \quad (n = 1, 2, \cdots;\ p \text{ 为素数}). \tag{9.3}$$

我们从这里便可以推出定理. 事实上, 在 (9.3) 中令 $n = p^k$, 则有

$$\tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1}) \quad (k = 1, 2, \cdots) \tag{9.4}$$

因此得到

$$\sum_{k=0}^{\infty}(\tau(p^k) - \tau(p)\tau(p^{k-1}) + p^{11}\tau(p^{k-2}))u^k = 1,$$

于是

$$\text{左端} = \left(\sum_{k=0}^{\infty}\tau(p^k)u^k\right)(1 - \tau(p)u + p^{11}u^2).$$

从而

$$\sum_{k=0}^{\infty}\tau(p^k)u^k = \frac{1}{1 - \tau(p)u + p^{11}u^2}. \tag{9.5}$$

特别地, $\tau(n)$ 具有乘性的性质 (即对于使得 $(m,n) = 1$ 的 m, n 有 $\tau(mn) = \tau(m)\tau(n)$) 可像下面那样由 (9.3) 得到. 为此只要证明

$$\text{如果 } p \nmid m \text{则 } \tau(p^k m) = \tau(p^k)\tau(m) \tag{9.6}$$

就可以了. 这可由对 k 的归纳进行证明. 当 $k=0$ 时这是显然的, 而 $k=1$ 时则是在 (9.3) 中取 $n=m$ 的结果. 现在设直到 k 其都成立. 在 (9.3) 中取 $n=p^k m$ 则有

$$\tau(p^{k+1}m)=\tau(p)\tau(p^k m)-p^{11}\tau(p^{k-1}m)$$

再由归纳法假定, 便有

$$\begin{aligned}\tau(p^{k+1}m) &= \tau(p)\tau(p^k)\tau(m)-p^{11}\tau(p^{k-1})\tau(m)\\ &= (\tau(p)\tau(p^k)-p^{11}\tau(p^{k-1}))\tau(m)\\ &\underset{(9.4)}{=} \tau(p^{k+1})\tau(m),\end{aligned}$$

故在 $k+1$ 时也成立, 从而 $\tau(n)$ 为乘性函数. 因此

$$\begin{aligned}\sum_{n=1}^{\infty}\tau(n)n^{-s} &= \prod_p(\sum_{k=0}^{\infty}(\tau(p^k)p^{-ks})\\ &= \prod_p(1-\tau(p)p^{-s}+p^{11-2s})^{-1}.\end{aligned}$$

(由这个推导可知, 定理中的等式等价于 $\tau(n)$ 为乘性函数以及 $\tau(p^k)$ 的递推公式 (9.4) 这两个联合条件.)

如此一来, 对定理 9.1 的证明只要能证明 $T(p)\Delta=\tau(p)\Delta$ 就好了. 我们说 Δ 为特征函数, 这一等式表明对于函数

$$f(z)=\frac{(T(p)\Delta)(z)}{\Delta(z)}$$

下面的两个条件成立:

(1) $f(z)$ 为常数函数,

(2) 这个常数等于 $\tau(p)$.

先看 (1). 如果能证明 $f(z)$ 对于所有的 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$ 满足

$$f\left(\frac{az+b}{cz+d}\right)=f(z)$$

即可. 知道了这一点以及 $SL_2(\mathbb{Z})\backslash H$ 的代表系(基本区域) 是如图 9.1 所示的阴影部分

$$\begin{aligned}D=&\left\{x+iy\,\middle|\,-\frac{1}{2}<x<\frac{1}{2},\ y>\sqrt{1-x^2}\right\}\\ &\sqcup\left\{-\frac{1}{2}+iy\,\middle|\,y>\frac{\sqrt{3}}{2}\right\}\sqcup\left\{x+i\sqrt{1-x^2}\,\middle|\,-\frac{1}{2}\leqslant x\leqslant 0\right\}\end{aligned}$$

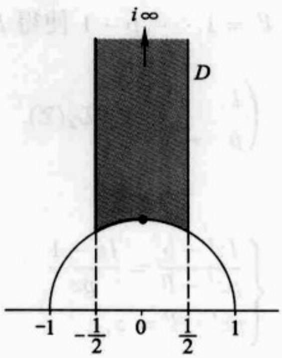


图 9.1

(这将用 $SL_2(\mathbb{Z})$ 由 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 和 $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ 生成的群论结果在 §9.6 中予以证明), 那么由于 $f(z)$ 在 $D=SL_2(\mathbb{Z})\backslash H$ 上全纯且在 $z=i\infty$ 也全纯, 那么根据复变函数论的 Liouville 定理 (极大值原理或者紧区域上的复变函数论) 知 $f(z)$ 为常数. 另一方面, 如前面的计算那样, 有

$$f(z)=\frac{(T(p)\Delta)(z)}{\Delta(z)}=\frac{\tau(p)q+(q^2\text{以上的项})}{q-24q^2+\cdots}=\frac{\tau(p)+(q\text{以上的项})}{1-24q+\cdots},$$

故当 $z\to i\infty\quad(q\to 0)$ 时 $f(z)\to\tau(p)$, 从而 $f(z)=\tau(p)$, (2) 得证.

那么, 因为 $\Delta(z)$ 满足变换公式

$$\Delta\left(\frac{az+b}{cz+d}\right)=(cz+d)^{12}\Delta(z)$$

(将在 §9.2 中证明), 要想证明 (1) 则只要能说明 $T(p)\Delta$ 满足同样的变换公式就好了. 这只要对于 $SL_2(\mathbb{Z})$ 的生成元 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 和 $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ 弄清楚这点就够了. 对于 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$, 由 Fourier 展开得到

$$(T(p)\Delta)(z+1)=(T(p)\Delta)(z),$$

而对于 $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$, 则像下面这样进行. 首先有

$$\begin{aligned}(T(p)\Delta)\left(-\frac{1}{z}\right)&=\frac{1}{p}\Delta\left(-\frac{1}{pz}\right)+p^{11}\Delta\left(-\frac{p}{z}\right)+\frac{1}{p}\sum_{l=1}^{p-1}\Delta\left(\frac{-\frac{1}{z}+l}{p}\right)\\&=\frac{1}{p}(pz)^{12}\Delta(pz)+p^{11}\left(\frac{z}{p}\right)^{12}\Delta\left(\frac{z}{p}\right)+\frac{1}{p}\sum_{l=1}^{p-1}\Delta\left(\frac{lz-1}{pz}\right).\end{aligned}$$

现在, 对于 $l=1,\cdots,p-1$ 取 $l'=1,\cdots,p-1$ 使得 $ll'\equiv -1 \mod p$(存在且唯一). 于是存在 b 使得

$$\begin{pmatrix} l & b \\ p & -l' \end{pmatrix} \in SL_2(\mathbb{Z}).$$

此时对于 $z'=\dfrac{z+l'}{p}$, 由于

$$\begin{cases} \dfrac{lz'+b}{pz'-l'} = \dfrac{lz-1}{pz} \\ pz'-l' = z, \end{cases}$$

故满足

$$\Delta\left(\frac{lz-1}{pz}\right) = z^{12}\Delta\left(\frac{z+l'}{p}\right).$$

于是得到

$$\begin{aligned}(T(p)\Delta)\left(-\frac{1}{z}\right) &= p^{11}z^{12}\Delta(pz) + \frac{1}{p}z^{12}\Delta\left(\frac{z}{p}\right) + \frac{1}{p}\sum_{l'=1}^{p-1} z^{12}\Delta\left(\frac{z+l'}{p}\right) \\ &= z^{12}(T(p)\Delta)(z).\end{aligned}$$

因此定理 9.1 得证. ∎

(b) Ramanujan 同余式

在此将证明 Ramanujan 的同余式 ③.

定理 9.2 (Ramanujan) 对于素数 p 成立

$$\tau(p) \equiv 1 + p^{11} \mod 691.$$

[证明] 更一般地, 我们可得到对于自然数 n 有

$$\tau(n) \equiv \sigma_{11}(n) \mod 691$$

的结论, 其中 $\sigma_k(n) = \sum\limits_{d|n} d^k$.

为此我们要用到**Eisenstein 级数** (Eisenstein series) $E_k(z)$. ($E_k(z)$ 的性质的证明将在 §9.2 中进行.) 当 k 为不小于 4 的偶数时,

$$E_k(z) = \frac{1}{2}\sum_{(c,d)=1}\frac{1}{(cz+d)^k}$$

绝对收敛, 它的 Fourier 展开为

$$E_k(z) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n \qquad (q=e^{2\pi iz}).$$

其中 $c, d \in \mathbb{Z}$ 取遍互素的整数组, B_k 为 Bernoulli 数

$$\frac{t}{e^t-1}=\sum_{k=0}^{\infty}\frac{B_k}{k!}t^k.$$

另外 $E_k(z)$ 还对于所有 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ 满足变换公式

$$E_k\left(\frac{az+b}{cz+d}\right)=(cz+d)^k E_k(z)$$

(具权 k 的自守性). 前面几个 $E_k(z)$ 为

$$E_4(z)=1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n$$

$$E_6(z)=1-504\sum_{n=1}^{\infty}\sigma_5(n)q^n$$

$$E_8(z)=1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n$$

$$E_{10}(z)=1-264\sum_{n=1}^{\infty}\sigma_9(n)q^n$$

$$E_{12}(z)=1+\frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n$$

$$E_{14}(z)=1-24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n.$$

那么, 由此我们知道存在整数 $c \equiv 65520 \mod 691$ 使得

$$E_{12}-E_6^2=\frac{c}{691}\Delta \tag{9.7}$$

成立. 与前一小节 $T(p)\Delta=\tau(p)\Delta$ 的证明完全一样地得到

$$\frac{E_{12}-E_6^2}{\Delta}=\frac{\left(\frac{65520}{691}+1008\right)q+(q\text{的大于等于2次的项})}{q+(q\text{的大于等于2次的项})}$$
$$=\frac{\left(\frac{65520}{691}+1008\right)+(q\text{的大于等于1次的项})}{1+(q\text{的大于等于1次的项})}$$

为 $SL_2(\mathbb{Z})$ 不变. 特别有

$$c=65520+1008\times 691=1008\times 756.$$

在 (9.7) 乘以 691 并对 q^n 项的系数的 mod 691 进行比较, 则得到

$$\sigma_{11}(n) \equiv \tau(n) \mod 691.$$

另外, 求出 (9.7) 的 q^n 的系数并比较就得出了 $\tau(n)$ 下面的公式

$$\begin{aligned} \tau(n) &= \frac{65}{756}\sigma_{11}(n) + \frac{691}{756}\sigma_5(n) - \frac{691}{3}\sum_{m=1}^{n-1}\sigma_5(m)\sigma_5(n-m) \\ &= \sigma_{11}(n) + \frac{691}{756}\left(-\sigma_{11}(n) + \sigma_5(n) - 252\sum_{m=1}^{n-1}\sigma_5(m)\sigma_5(n-m)\right). \end{aligned} \tag{9.8}$$

自然, 一眼就可看出

$$\tau(n) \equiv \sigma_{11}(n) \mod 691$$

了. ∎

(c) Ramanujan 等式与 Lambert 级数

下面形式的级数称为 Lambert 级数, 它对于自守形式的表示提供了一些方便:

$$\sum_{n=1}^{\infty}\frac{a(n)q^n}{1-q^n}.$$

可以将其变形为 Fourier 级数 (q 的幂级数)

$$\sum_{n=1}^{\infty}\frac{a(n)q^n}{1-q^n} = \sum_{n=1}^{\infty}a(n)\left(\sum_{m=1}^{\infty}q^{mn}\right) = \sum_{n,m=1}^{\infty}a(n)q^{mn} = \sum_{l=1}^{\infty}\left(\sum_{n|l}a(n)\right)q^l$$

(最后那个等式将 mn 换成了 l, 从而加上了相应的条件 $n|l$).

具有代表性的是 Eisenstein 级数 $E_k(z)$ 的 Fourier 展开

$$\sum_{n=1}^{\infty}\frac{n^{k-1}q^n}{1-q^n} = \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

因此,

$$E_k(z) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\frac{n^{k-1}q^n}{1-q^n}. \tag{9.9}$$

另外, 对于 Euler 函数 $\varphi(n)$ 以及 Möbius 函数 $\mu(n)$ 的情形也有

$$\sum_{n=1}^{\infty}\frac{\varphi(n)q^n}{1-q^n} = \sum_{n=1}^{\infty}nq^n = \frac{q}{(1-q)^2},$$

$$\sum_{n=1}^{\infty}\frac{\mu(n)q^n}{1-q^n} = q.$$

它们各自表明的意思是

$$\sum_{m|n}\varphi(m)=n,$$

$$\sum_{m|n}\mu(m)=\begin{cases}1 & n=1\\ 0 & n\geqslant 2.\end{cases}$$

另一方面, 如果给出了 Fourier 级数, 则可将其改写为 Lambert 级数:

$$\sum_{n=1}^{\infty}A(n)q^n=\sum_{n=1}^{\infty}\left(\sum_{m|n}\mu\left(\frac{n}{m}\right)A(m)\right)\frac{q^n}{1-q^n}.$$

这个变换是 Möbius(逆) 变换:

$$A(n)=\sum_{m|n}a(m)\quad\Longleftrightarrow\quad a(n)=\sum_{m|n}\mu\left(\frac{n}{m}\right)A(m).$$

Ramanujan 是个著名的擅长计算的人, 尤其喜好求 Lambert 级数的值, 留下了许多这方面计算的手稿 (以亲自写的笔记的誊写版出版). 现举出其中的几个.

定理 9.3 (Ramanujan 的等式)

(1) $\displaystyle\sum_{n=1}^{\infty}\frac{n^5}{e^{2\pi n}-1}=\frac{1}{504}.$

(2) $\displaystyle\sum_{n=1}^{\infty}\frac{n}{e^{2\pi n}-1}=\frac{1}{24}-\frac{1}{8\pi}.$

(3) $\displaystyle\sum_{n=1}^{\infty}\frac{n^3}{e^{2\pi n}-1}=\frac{\Gamma\left(\frac{1}{4}\right)^8}{5120\pi^6}-\frac{1}{240}=\frac{1}{80}\left(\frac{\varpi}{\pi}\right)^4-\frac{1}{240}.$

[证明] (1) 根据 $E_6(z)$ 的变换公式有

$$E_6\left(-\frac{1}{z}\right)=z^6E_6(z),$$

在其中代入 $z=i$ 则成立

$$E_6(i)=i^6E_6(i)=-E_6(i),$$

故 $E_6(i)=0$. 另一方面, 按照 Fourier 展开有

$$\begin{aligned}E_6(i)&=1-504\sum_{n=1}^{\infty}\sigma_5(n)e^{-2\pi n}=1-504\sum_{n=1}^{\infty}\frac{n^5e^{-2\pi n}}{1-e^{-2\pi n}}\\&=1-504\sum_{n=1}^{\infty}\frac{n^5}{e^{2\pi n}-1}.\end{aligned}$$

从而得到 (1). (2), (3) 的证明以后进行 (§9.5). ∎

(d) Ramanujan 的手稿

Ramanujan 在其未发表的手稿 (推测在 1916 年左右) 中不止是考虑了 $L(s,\Delta)$, 在

$$F(z)=q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2=\sum_{n=1}^{\infty}c(n)q^n$$

的情形还考虑了

$$L(s,F)=\sum_{n=1}^{\infty}c(n)n^{-s},$$

并猜想

$$L(s,F)=(1-c(11)11^{-s})^{-1}\times\prod_{p\neq 11}(1-c(p)p^{-s}+p^{1-2s})^{-1}.$$

在这里的 $c(11)=1$. 这个 L 函数的关于 11 的因子为一次式, 这是与 $L(s,\Delta)$ 不同的一点. $F(z)$ 并不是 $SL_2(\mathbb{Z})$ 的自守形式, 而是成为关于 $SL_2(\mathbb{Z})$ 的子群

$$\Gamma_0(11)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})\,\middle|\, c\equiv 0 \mod 11\right\}$$

有变换公式

$$F\left(\frac{az+b}{cz+d}\right)=(cz+d)^2F(z)$$

的权为 2 的自守形式.

差不多 40 年后, Eichler(1954年) 才证明了 $L(s,F)$ 与 $\mathbb{Q}$ 上的椭圆曲线

$$E: y^2+y=x^3-x^2$$

的 L 函数 $L(s,E)$ 一致. 这又是在差不多半个世纪后跨出的一大步, 从而到达了 Fermat 大定理的证明 (Wiles, 1995年). Wiles 的证明是由对于非常多的椭圆曲线 E 都成立形如 $L(s,E)=L(s,F)$ 的等式这个结果推导出来的 (参照第十二章).

另外, Ramanujan 还证明了同余式

$$\tau(p)\equiv c(p) \mod 11. \tag{9.10}$$

将 F 与 Δ 都看成是 $\mathbb{Z}$ 系数的 q 的形式幂级数 (即 $\mathbb{Z}[[q]]$ 的元) 时, 由取 mod 11 有

$$\begin{aligned}F&=q\prod_{n=1}^{\infty}(1-q^n)^2\cdot[(1-q^{11n})]^2\\&\equiv q\prod_{n=1}^{\infty}(1-q^n)^2\cdot[(1-q^n)^{11}]^2\\&=\Delta \mod 11,\end{aligned}$$

从而看出同余式成立. 定理 9.2 的同余式是权同为 12 的自守形式 Δ 与 E_{12} 之间的同余式, 而 Δ 与 F 这样不同权的自守形式间的同余式也是重要的.

(e) Ramanujan 猜想的后继结果

Ramanujan 猜想 (1916 年)

$$|\tau(p)| < 2p^{\frac{11}{2}}$$

的证明, 经过 Grothendieck 对代数几何的革新 (20 世纪 60 年代)之后, 在 1974 年由 Deligne 所完成. 于是, 对于各个素数 p 存在唯一一个 $0 < \theta_p < \pi$ 使得

$$\tau(p) = 2p^{\frac{11}{2}} \cos\theta_p$$

成立.

在 Ramanujan 猜想之后继续要做的是详细分析 θ_p. (这与在 Riemann 猜想被证明之后, 变成详细分析零点虚部的问题是平行的. Ramanujan 猜想与 Riemann 猜想在这方面是类似的.) 在这个方向上, 有 1962 年左右由佐藤干夫提出并由 J.Tate 给予其代数几何解释的佐藤 –Tate 猜想. (在那时, Ramanujan 猜想还没得到证明, 然而佐藤的研究弄清了 Ramanujan 猜想与 Riemann 猜想的类似性, 故而达到了以下的猜想.)

佐藤 – Tate 猜想 对于 $0 \leqslant \alpha < \beta \leqslant \pi$ 的 α, β, 有

$$\lim_{x\to\infty} \frac{\#\{p \leqslant x \mid \alpha \leqslant \theta_p \leqslant \beta\}}{\pi(x)} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta d\theta.$$

这个猜想说的是 θ_p 集中在 $\pi/2$ 附近. $\pi(x)$ 表示小于 x 的素数的个数, 而猜想的右端是 θ_p 落入 $[\alpha,\beta]$ 的期待概率. 当然, 我们有

$$\frac{2}{\pi}\int_0^\pi \sin^2\theta d\theta = 1.$$

(图9.2).

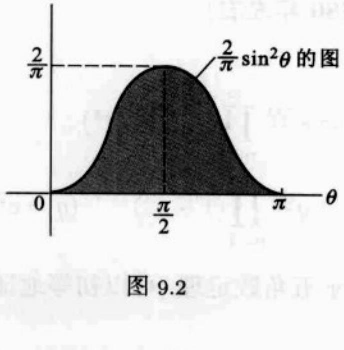


图 9.2

佐藤 -Tate 猜想被看成是对于 Δ 的"素数定理的类比"的一个基本猜想, 迄今为止还没有被证明. 然而, 在对它的研究过程中, 不仅仅有

$$L(s,\Delta)=\prod_p(1-\tau(p)p^{-s}+p^{11-2s})^{-1}$$
$$=\prod_p[(1-\alpha_p p^{-s})(1-\beta_p p^{-s})]^{-1},$$

而且我们还知道, 如果对于 $m=1,2,3,\cdots$ 知道了 $m+1$ 次 Euler 积 (m 次对称积)

$$L(s,\mathrm{Sym}^m\Delta)=\prod_p[(1-\alpha_p^m p^{-s})(1-\alpha_p^{m-1}\beta_p p^{-s})\cdots(1-\alpha_p\beta_p^{m-1}p^{-s})(1-\beta_p^m p^{-s})]^{-1}$$

的解析性质, 那么就能够证明佐藤 -Tate 猜想了. 这些必需的解析性质包含在关于一般的自守形式 ζ 的 Langlands 猜想之中. 虽然期待这个猜想必定会成立, 但至今也只了解了 m 较小时的情形 (m=1, 2, 3, 4). $m=1$ 的情形可参看 §9.3(a), $m=2$ 的情形参看 §9.4(c).

§9.2 Ramanujan 的 Δ 与正则 Eisenstein 级数

(a) Ramanujan 的 Δ

在这里我们来证明 Δ 的变换公式.

定理 9.4 对于 $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$ 成立

$$\Delta\left(\frac{az+b}{cz+d}\right)=(cz+d)^{12}\Delta(z).$$

[证明] 因为这是个重要的事实, 我们介绍四种证明方法. 每一个都有不同的背景, 从而我们知道 Δ 处于自守形式理论的中心, 也看出了自守形式的多彩多姿.

方法 1 (Dedekind, 1880 年左右)

对如下定义的

$$\eta(z)=e^{\frac{\pi iz}{12}}\prod_{n=1}^{\infty}(1-e^{2\pi inz})$$
$$=q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)\qquad(q=e^{2\pi iz})$$

的 Dedekind η 函数, 由 Euler 五角数定理 (可以初等地证明) 得到

$$\eta(z) = q^{\frac{1}{24}} \sum_{m=-\infty}^{\infty} (-1)^m q^{\frac{m(3m-1)}{2}} = \sum_{m=-\infty}^{\infty} (-1)^m q^{\frac{(6m-1)^2}{24}} = \sum_{n=1}^{\infty} \chi(n) q^{\frac{n^2}{24}}, \tag{9.11}$$

然后应用被称为 ϑ 的自守形式的右端来给出定理的证明.

χ 是 mod 12 的 (本原) 偶特征, 对其定义为

$$\chi(n) = \begin{cases} 1 & m \equiv \pm 1 \mod 12 \\ -1 & n \equiv \pm 5 \mod 12 \\ 0 & \text{其他}. \end{cases}$$

它的 Gauss 和 $G(\chi) = 2\sqrt{3}$. 若以 §7.2(b) 的记号表示, 我们则有 $\eta(iy) = \psi_\chi(y)$, 且由 Poisson 求和公式 (参看 §11.2) 推导出 $\psi_\chi(y)$ 的变换公式为

$$\psi_\chi\left(\frac{1}{y}\right) = \sqrt{y}\psi_\chi(y),$$

从而

$$\eta\left(i\frac{1}{y}\right) = \sqrt{y}\eta(iy).$$

因此成立

$$\eta\left(-\frac{1}{z}\right) = \sqrt{\frac{z}{i}}\eta(z)$$

(它的两边都在上半平面为全纯, 由于在虚轴上相等故在上半平面相等). 作 24 次乘方得到

$$\Delta\left(-\frac{1}{z}\right) = z^{12}\Delta(z).$$

这是对于 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$ 的变换, 又因为对 $SL_2(\mathbb{Z})$ 的另一个生成元 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 的变换

$$\Delta(z+1) = \Delta(z)$$

是显然成立的, 故对于所有的 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ 成立

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z).$$

方法 2 (Kronecker, 1890 年左右)

根据 Kronecker 极限公式 (在 §9.5 证明) 知 $\mathrm{Im}(z)^6|\Delta(z)| = y^6|\Delta(z)|$ 为 $SL_2(\mathbb{Z})$ 不变 (§9.5(d)). 特别地有

$$y^6|\Delta(iy)| = \left(\frac{1}{y}\right)^6 \left|\Delta\left(i\frac{1}{y}\right)\right|.$$

由于上式的绝对值里是全为正的实数, 故

$$y^6\Delta(iy) = y^{-6}\Delta\left(i\frac{1}{y}\right),$$

即

$$\Delta\left(-\frac{1}{iy}\right) = (iy)^{12}\Delta(iy).$$

于是推出了

$$\Delta\left(-\frac{1}{z}\right) = z^{12}\Delta(z).$$

方法 3 (Siegel, 1954年)

对于 $t>0$ 证明

$$\eta\left(i\frac{1}{t}\right) = \sqrt{t}\eta(it),$$

并在两边作 24 次乘方即可. 为此, 对其两边取对数, 有

$$\log\eta\left(i\frac{1}{t}\right) = \frac{1}{2}\log t + \log\eta(it)$$

它等价于

$$-\frac{\pi t - \pi t^{-1}}{12} + \frac{1}{2}\log t = \sum_{k=1}^{\infty}\frac{1}{k}\left(\frac{1}{e^{2\pi kt}-1} - \frac{1}{e^{2\pi kt^{-1}}-1}\right). \tag{9.12}$$

现在对于 $n=0,1,2,\cdots$ 令 $\nu = \left(n+\frac{1}{2}\right)\pi$, 我们对函数

$$f_\nu(z) = \frac{1}{2}\cot(\nu z)\cot\left(\frac{\nu z}{it}\right)$$

计算留数

$$\frac{1}{2\pi i}\int_C f_\nu(z)d = \sum_{z:C\text{内部的极点}} \mathrm{Res}_z(f_\nu).$$

其中 C 为图 9.3 的菱形 (× 表示极点).

极点与留数列于下:

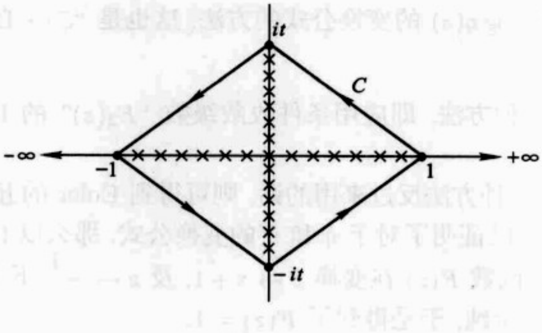


图 9.3

$$\begin{cases} z = \pm\dfrac{\pi k}{\nu} \quad (k=1,\cdots,n): & \text{一阶极点且}\mathrm{Res}_z(f_\nu) = \dfrac{1}{\pi k}\cot\left(\dfrac{\pi k}{it}\right) \\ z = \pm i\dfrac{\pi k t}{\nu} \quad (k=1,\cdots,n): & \text{一阶极点且}\mathrm{Res}_z(f_\nu) = \dfrac{1}{\pi k}\cot(i\pi k t) \\ z = 0: & \text{三阶极点且}\mathrm{Res}_0(f_\nu) = -\dfrac{1}{3}\left(it + \dfrac{1}{it}\right). \end{cases}$$

于是得到

$$\begin{aligned} -\frac{\pi t - \pi t^{-1}}{12} + \frac{1}{8}\int_C f_\nu(z)dz &= \frac{i}{2}\sum_{k=1}^{n}\frac{1}{k}\left(\cot(\pi i k t) + \cot\left(\frac{\pi k}{it}\right)\right) \\ &= \sum_{k=1}^{n}\frac{1}{k}\left(\frac{1}{e^{2\pi k t}-1} - \frac{1}{e^{2\pi k t^{-1}}-1}\right). \end{aligned}$$

在其中令 $n\to\infty$ 则

$$\begin{aligned} \text{左端} \to &-\frac{\pi t - \pi t^{-1}}{12} + \left(\int_1^{it} - \int_{it}^{-1} + \int_{-1}^{-it} - \int_{-it}^{1}\right)\frac{dz}{8z} \\ &= -\frac{\pi t - \pi t^{-1}}{12} + \frac{1}{2}\log t, \\ \text{右端} \to &\sum_{k=1}^{\infty}\frac{1}{k}\left(\frac{1}{e^{2\pi k t}-1} - \frac{1}{e^{2\pi k t^{-1}}-1}\right), \end{aligned}$$

从而得到了 (9.12), 因此给出了 η 的变换公式.

方法 4 (Weil, 1968 年)

这是由对于

$$\log\eta(z) = \log\left(q^{\frac{1}{24}}\right) + \sum_{n=1}^{\infty}c(n)q^n$$

的函数方程

$$\sum_{n=1}^{\infty}c(n)n^{-s} = -\zeta(s)\zeta(s+1)$$

在 $s \leftrightarrow -s$ 所得到的 $\log\eta(z)$ 的变换公式的方法, 这也是 "$\zeta \leftrightarrow$ 自守形式" 的一个示例 (参看 §9.3(b)).

注记 还有第五种方法, 即应用条件收敛级数 "$E_2(z)$" 的 Hurwitz 方法 (参看 §9.5(e)).

再说一点, 将第一种方法反过来用的话, 则可得到 Euler 的五角数定理的自守形式证明. 就是说, 如果已证明了对于 η 和 ϑ 的变换公式, 那么以 (9.11) 左端的 (η) 去除右端的 (ϑ) 得到的函数 $F(z)$ 在变换 $z \mapsto z+1$, 及 $z \mapsto -\dfrac{1}{z}$ 下不变, 那么应用其在 $SL_2(\mathbb{Z})\backslash H \cup \{i\infty\}$ 上全纯, 于是得到了 $F(z)=1$.

(b) 正则 Eisenstein 级数

我们来证明

$$E_k(z) = \frac{1}{2}\sum_{(c,d)=1} \frac{1}{(cz+d)^k}$$

的基本性质. 设 k 为不小于 4 的偶数. 首先只要代入上式便知有

$$E_k(z+1) = E_k(z)$$

和

$$E_k\left(-\frac{1}{z}\right) = z^k E_k(z):$$

$$E_k(z+1) = \frac{1}{2}\sum_{(c,d)=1} \frac{1}{(c(z+1)+d)^k} = \frac{1}{2}\sum_{(c,d)=1} \frac{1}{(cz+(c+d))^k} = E_k(z).$$

$$E_k(-\frac{1}{z}) = \frac{1}{2}\sum_{(c,d)=1} \frac{1}{\left(-c\dfrac{1}{z}+d\right)^k} = \frac{1}{2}\sum_{(c,d)=1} \frac{z^k}{(dz-c)^k} = z^k E_k(z).$$

因此, 对于 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ 有

$$E_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k E_k(z).$$

(直接代入计算也可即知.) 下面, 我们来计算其 Fourier 展开. 先从

$$\sin(\pi z) = \pi z \prod_{n=1}^{\infty}\left(1 - \frac{z^2}{n^2}\right)$$

出发. 对两端做对数微分 (即取对数再微分) 有

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2-n^2} = \frac{1}{z} + \sum_{n=1}^{\infty}\left(\frac{1}{z-n} + \frac{1}{z+n}\right).$$

现在取 $\mathrm{Im}(z) > 0$, 并令 $q = e^{2\pi iz}$, 则由于

$$\pi\cot(\pi z) = \pi\frac{\cos(\pi z)}{\sin(\pi z)} = \pi\frac{\left(\dfrac{e^{i\pi z}+e^{-i\pi z}}{2}\right)}{\left(\dfrac{e^{i\pi z}-e^{-i\pi z}}{2i}\right)}$$
$$= i\pi\frac{q+1}{q-1} = i\pi\left(1+\frac{2}{q-1}\right),$$

因此

$$-i\pi - 2i\pi\sum_{n=1}^{\infty} q^n = i\pi\left(1+\frac{2}{q-1}\right) = \frac{1}{z} + \sum_{n=1}^{\infty}\left(\frac{1}{z+n}+\frac{1}{z-n}\right). \tag{9.13}$$

对其两端取 $k-1$ 次微分则有

$$-(2\pi i)^k\sum_{n=1}^{\infty} n^{k-1}q^n = (-1)^{k-1}(k-1)!\sum_{n=-\infty}^{\infty}(z-n)^{-k},$$

即有

$$\sum_{n=-\infty}^{\infty}(z-n)^{-k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1}q^n. \tag{9.14}$$

(它被称为 Lipschitz 公式, 也可应用 Poisson 求和公式得到: 参看 §11.2.) 然而由于

$$\sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty}(mz+n)^{-k} = \sum_{l=1}^{\infty}\sum_{(c,d)=1}(lcz+ld)^{-k}$$
$$= \sum_{l=1}^{\infty} l^{-k}\sum_{(c,d)=1}(cz+d)^{-k},$$

故有

$$\begin{aligned}
E_k(z) &= \frac{1}{2\zeta(k)}\sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty}(mz+n)^{-k} \\
&= \frac{1}{2\zeta(k)}\sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} n^{-k} + \frac{1}{\zeta(k)}\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}(mz+n)^{-k} \\
&= 1 + \frac{1}{\zeta(k)}\sum_{m=1}^{\infty}\left(\sum_{n=-\infty}^{\infty}(mz+n)^{-k}\right) \\
&\underset{(9.14)}{=} 1 + \frac{1}{\zeta(k)}\sum_{n=1}^{\infty}\frac{(2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty} n^{k-1}q^{mn} \\
&= 1 + \frac{1}{\zeta(k)}\sum_{n=1}^{\infty}\frac{(2\pi i)^k}{(k-1)!}\sigma_{k-1}(n)q^n.
\end{aligned}$$

因为其中

$$\zeta(k) = -\frac{(2\pi i)^k}{2\cdot k!}B_k \tag{9.15}$$

从而

$$E_k(z) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

同时我们注意到, 应用第三章的推论 3.22 的

$$\zeta(1-k) = -\frac{B_k}{k},$$

可以将其写为

$$E_k(z) = 1 + \frac{2}{\zeta(1-k)}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n. \tag{9.16}$$

再有, 我们知道 (9.15) 由 $\zeta(1-k)$ 的函数方程 $\zeta(k) \leftrightarrow \zeta(1-k)$ (第七章的定理 7.1) 得到, 然而由 (9.13) 却可以立刻将它写出来: 因为

$$\begin{aligned}\pi i\left(1+\frac{2}{q-1}\right) &= \frac{1}{z} + \sum_{n=1}^{\infty}\frac{2z}{z^2-n^2}\\ &= \frac{1}{z} - \sum_{n=1}^{\infty}\frac{\frac{2z}{n^2}}{1-\frac{z^2}{n^2}} = \frac{1}{z} - \frac{2}{z}\sum_{n=1}^{\infty}\frac{\frac{z^2}{n^2}}{1-\frac{z^2}{n^2}}\\ &= \frac{1}{z} - \frac{2}{z}\sum_{n=1}^{\infty}\sum_{l=1}^{\infty}\left(\frac{z^2}{n^2}\right)^l = \frac{1}{z} - \frac{2}{z}\sum_{l=1}^{\infty}\zeta(2l)z^{2l},\end{aligned}$$

而由 Bernoulli 数的定义有

$$\pi i\left(1+\frac{2}{q-1}\right) = \pi i + \frac{2\pi i}{e^{2\pi i z}-1} = \pi i + \frac{1}{z}\sum_{l=0}^{\infty}\frac{B_l}{l!}(2\pi i z)^l,$$

故得到了

$$-\zeta(2l) = \frac{1}{2}\frac{B_{2l}(2\pi i)^{2l}}{(2l)!}.$$

(c) Δ 与正则 Eisenstein 级数的关系

定理 9.5

$$\Delta = \frac{E_4^3 - E_6^2}{1728}.$$

[证明]

当令

$$f(z) = \frac{E_4(z)^3 - E_6(z)^2}{\Delta(z)}$$
$$= \frac{1728q + (q\text{的大于等于2次项})}{q + (q\text{的大于等于2次项})} = \frac{1728 + (q\text{的大于等于1次项})}{1 + (q\text{的大于等于1次项})}$$

时, 如果能断定 $f(z)$ 为常值函数, 则取 $z \to i\infty$ $(q \to 0)$ 便知 $f(z) = 1728$.

至于证明其为常值函数则与 §9.1(a), (b) 完全一样, 从 $f(z)$ 为 $SL_2(\mathbb{Z})$ 不变得到. ∎

推论 9.6

$$E_4(i) = 12\Delta(i)^{\frac{1}{3}}.$$

[证明] 在定理 9.5 中代入 $z = i$, 则由 $E_6(i) = 0$ 得到

$$E_4(i)^3 = 1728\Delta(i) = 1728e^{-2\pi}\prod_{n=1}^{\infty}(1 - e^{-2\pi n})^{24} > 0.$$

将其开三次方即得. ∎

§9.3 自守性与 ζ 的函数方程

(a) Wilton 的结果

Wilton(1929 年) 得到了由 Δ 构造的 ζ 函数 $L(s, \Delta)$:

$$L(s, \Delta) = \prod_{p}(1 - \tau(p)p^{-s} + p^{11-2s})^{-1}$$
$$= \sum_{n=1}^{\infty}\tau(n)n^{-s}$$

的解析延拓和函数方程.

定理 9.7 (Wilton) $L(s, \Delta)$ 可解析延拓为全复平面上的全纯函数. 另外,

$$\widehat{L}(s, \Delta) = (2\pi)^{-s}\Gamma(s)L(s, \Delta)$$

满足函数方程

$$\widehat{L}(s, \Delta) = \widehat{L}(12 - s, \Delta).$$

[证明] 由 Γ 函数的定义

$$\Gamma(s)=\int_0^\infty e^{-x}x^{s-1}dx \qquad (\mathrm{Re}\,(s)>0),$$

对于 $n=1,2,3,\cdots$ 有

$$(2\pi)^{-s}\Gamma(s)n^{-s}=\int_0^\infty e^{-2\pi ny}y^{s-1}dy.$$

因此有

$$\begin{aligned}\widehat{L}(s,\Delta)&=\int_0^\infty\left(\sum_{n=1}^\infty\tau(n)e^{-2\pi ny}\right)y^{s-1}dy\\&=\int_0^\infty\Delta(iy)y^{s-1}dy\\&=\int_0^1\Delta(iy)y^{s-1}dy+\int_1^\infty\Delta(iy)y^{s-1}dy\\&=\int_1^\infty\Delta\left(i\frac{1}{y}\right)y^{-s-1}dy+\int_1^\infty\Delta(iy)y^{s-1}dy\\&=\int_1^\infty(\Delta(iy)y^{12})y^{-s-1}dy+\int_1^\infty\Delta(iy)y^{s-1}dy\\&=\int_1^\infty\Delta(iy)(y^{12-s}+y^s)\frac{dy}{y},\end{aligned}$$

从而得到了其在全平面上的全纯性与函数方程. 更进一步说, 由于有对于 $\tau(n)$ 的增大速度的结果

$$\tau(n)=O(n^6), \tag{9.17}$$

我们还知道, $L(s,\Delta)$ 在 $\mathrm{Re}\,(s)>7$ 时绝对收敛. 这个增大结果可按如下证明. 因为 $y^6|\Delta(z)|$ 在 $SL_2(\mathbb{Z})\backslash H\cup\{i\infty\}$ 上连续 (成为紧空间上的连续函数) 故而有界, 从而存在 $M>0$ 使得

$$y^6|\Delta(z)|\leqslant M.$$

另一方面, 因为

$$\int_{-\frac{1}{2}}^{\frac{1}{2}}\Delta(x+iy)e^{-2\pi inx}dx=\tau(n)e^{-2\pi ny},$$

那么令 $y=\dfrac{1}{n}$ 则有

$$\tau(n)e^{-2\pi}=\int_{-\frac{1}{2}}^{\frac{1}{2}}\Delta\left(x+i\frac{1}{n}\right)e^{-2\pi inx}dx.$$

于是

$$|\tau(n)|\leqslant e^{2\pi}\int_{-\frac{1}{2}}^{\frac{1}{2}}\left|\Delta\left(x+i\frac{1}{n}\right)\right|dx\leqslant Me^{2\pi}n^6$$

即

$$\tau(n) = O(n^6).$$ □

注记 Wilton 证明了 $L(s,\Delta)$ 及 $\widehat{L}(s,\Delta)$ 在函数方程 $s \leftrightarrow 12-s$ 的中心轴 $\mathrm{Re}\,(s)=6$ 上有无限多个零点. 这是接近于这一情形下的 Riemann 猜想 "$\widehat{L}(s,\Delta)$ 的零点全在直线 $\mathrm{Re}(s)=6$ 上" 的结果.

(b) Hecke 的逆定理

Hecke(1936 年) 考虑了 Wilton 定理的逆: $L(s,\Delta)$ 是被函数方程特征刻画的吗? 答案是肯定的. 为了说明这一点, 我们从 Wilton 定理的证明中注意到, $\widehat{L}(s,\Delta)$ 在各个竖直区域 $\sigma_1 \leqslant \mathrm{Re}\,(s) \leqslant \sigma_2$ 中有界 (图 9.4):

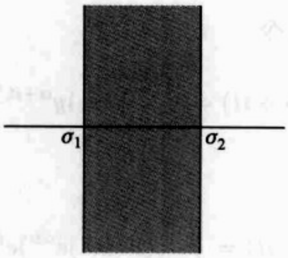


图 9.4

$$\begin{aligned}|\widehat{L}(s,\Delta)| &\leqslant \int_1^\infty \Delta(iy)(y^{\mathrm{Re}(s)}+y^{12-\mathrm{Re}(s)})\frac{dy}{y}\\ &\leqslant \int_1^\infty \Delta(iy)(y^{\sigma_2}+y^{12-\sigma_1})\frac{dy}{y}.\end{aligned}$$

定理 9.8 (Hecke) 对于复数序列 $\boldsymbol{a}=(a(1),a(2),a(3),\cdots)$ 令

$$L(s,\boldsymbol{a}) = \sum_{n=1}^\infty a(n)n^{-s},$$
$$\widehat{L}(s,\boldsymbol{a}) = (2\pi)^{-s}\Gamma(s)L(s,\boldsymbol{a}).$$

那么, 下面的 (A) 与 (B) 等价:

(A) $a(n)=\tau(n) \quad (n=1,2,3,\cdots)$.

(B) (1) $a(1)=1$.

(2) 对于某个 $\gamma>0$ 有 $a(n)=O(n^\gamma)$.

(3) $\widehat{L}(s,\boldsymbol{a})$在整个 s 平面全纯, 且 $\widehat{L}(12-s,\boldsymbol{a})=\widehat{L}(s,\boldsymbol{a})$.

(4) $\widehat{L}(s,\boldsymbol{a})$在各竖直区域有界.

[证明]　(A) ⇒(B) 已经知道了. 来证明 (B)⇒(A). 为简单计, 记 $\varphi(s) = L(s, \boldsymbol{a})$, $\Phi(s) = \widehat{L}(s, \boldsymbol{a})$. 我们注意到, 根据 (B–2), $\varphi(s)$ 在 $\mathrm{Re}\,(s) > \gamma + 1$ 上绝对收敛. 现令

$$F(z) = \sum_{n=1}^{\infty} a(n) q^n,$$

于是有

$$\Phi(s) = \int_0^{\infty} F(iy) y^{s-1} dy.$$

在此施行 Fourier 逆变换 (Mellin 逆变换) 则

$$F(iy) = \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} \Phi(s) y^{-s} ds$$

对于 $\alpha > \gamma + 1$ 成立. 实际上, 令

$$\Phi(\alpha + it) = \int_0^{\infty} F(iy) y^{\alpha + it} \frac{dy}{y},$$

并作替换 $y = e^u$, 于是有

$$\Phi(\alpha + it) = \int_{-\infty}^{\infty} (F(ie^u) e^{\alpha u}) e^{itu} du,$$

那么, 因为由通常的 Fourier 逆变换有

$$F(ie^u) e^{\alpha u} = \frac{1}{2\pi} \int_{-\infty}^{\infty} \Phi(\alpha + it) e^{-itu} dt,$$

故而得到了

$$F(iy) = \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} \Phi(s) y^{-s} ds.$$

沿着图 9.5 的积分路径移动, 并设 $T \to +\infty$,

于是我们有

$$\begin{aligned}
F(iy) &\underset{(\text{B}-4)}{=} \frac{1}{2\pi i} \int_{12-\alpha - i\infty}^{12-\alpha + i\infty} \Phi(s) y^{-s} ds \\
&= \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} \Phi(12 - s) y^{-(12-s)} ds \\
&\underset{(\text{B}-3)}{=} \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} \Phi(s) y^{s-12} ds \\
&= y^{-12} \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} \Phi(s) \left(\frac{1}{y}\right)^{-s} ds \\
&= y^{-12} F\left(i \frac{1}{y}\right).
\end{aligned}$$

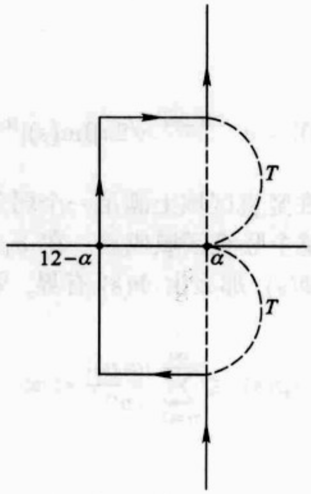


图 9.5

也就是说, 有

$$F\left(i\frac{1}{y}\right) = y^{12}F(iy),$$

由此便得到了

$$F\left(-\frac{1}{z}\right) = z^{12}F(z).$$

因此, 由 (B–1) 有 $a(1) = 1$, 故而

$$\frac{F(z)}{\Delta(z)} = \frac{q + a(2)q^2 + \cdots}{q + \tau(2)q^2 + \cdots} = \frac{1 + a(2)q + \cdots}{1 + \tau(2)q + \cdots}$$

为 $SL_2(\mathbb{Z})$ 不变, 从而在基本区域上 (包含了 $i\infty$) 为全纯, 故为常值, 并取 $z \to i\infty$ 得常数为 1. 所以 $F(z) = \Delta(z)$, 于是 $a(n) = \tau(n)$.

进一步我们需注意, 要看出在上述积分路径平行移动时在与实轴平行部分上的积分当 $T \to +\infty$ 时趋向 0, 必须使用条件 (B–4) , 并且还需用到下面的两个结果:

(PL) Phragmén-Lindelöf 定理:

设在 $\sigma_1 \leqslant \mathrm{Re}\,(s) \leqslant \sigma_2$ 中的全纯函数 $\Phi(s)$ 对于某个常数 μ 满足下面的条件: 当 $|\mathrm{Im}(s)| \to \infty$ 时有

$$\Phi(s) = O\left(e^{|\mathrm{Im}(s)|^{\mu}}\right),$$

且在 $\mathrm{Re}\,(s) = \sigma_1, \sigma_2$ 上, 当 $|\mathrm{Im}(s)| \to \infty$ 时存在常数 M 使得

$$\Phi(s) = O(|\mathrm{Im}(s)|^{M}).$$

于是此时在 $\sigma_1 \leqslant \mathrm{Re}\,(s) \leqslant \sigma_2$ 时成立

$$\Phi(s) = O(|\mathrm{Im}(s)|^{M}).$$

(S) Stirling 公式

当$|\mathrm{Im}(s)| \to \infty$ 时成立

$$|\Gamma(s)| \sim e^{-\frac{\pi|\mathrm{Im}(s)|}{2}}\sqrt{2\pi}|\mathrm{Im}(s)|^{\mathrm{Re}\,(s)}.$$

(PL) 说的是, 某个函数在竖直区域上满足一个弱条件, 但在边界上如果成立一个强条件, 则此强条件便在整个竖直区域成立. 在 $\sigma_1 = 12 - \alpha$, $\sigma_2 = \alpha$ 的情形, 将 (PL) 应用于最初的那个 $\Phi(s)$, 那么由 $\Phi(s)$ 有界, 又取 $\mu = 0$, 则根据 (B–2), 在 $\mathrm{Re}\,(s) = \sigma_2 = \alpha$ 上便有

$$|\varphi(s)| \leqslant \sum_{n=1}^{\infty} \frac{|a(n)|}{n^{\alpha}} < \infty,$$

于是应用 (S) 则有

$$\Phi(s) = O(\mathrm{Im}(s)|^{-1})$$

(更进一步是 $O\left(e^{-c|\mathrm{Im}(s)|}\right)$ 这样的形式), 这样, 根据函数方程 (B–3) 知该估值在 $\mathrm{Re}\,(s) = \sigma_1 = 12 - \alpha$ 上也成立. 因此可应用 (PL) 于 $M = -1$. 所以积分路径可以平行移动. ∎

定理 9.8 所说的是, 成立下面的对应关系

$$F \text{ 的自守性} \longleftrightarrow \Phi \text{ 的函数方程}.$$

在 §7.2(a) 所使用过的关系式

$$\vartheta(z) \longleftrightarrow \zeta(s)$$

以及在 §9.2 (a) 所用过的方法 4

$$\log \eta(z) \longleftrightarrow \zeta(s)\zeta(s+1)$$

等等, 都是类似的例子. 还有, 上面给出的定理 9.8 中数 12 是重要的. 譬如将其换作 8 时, 我们已知并不存在满足 (B–1)—(B–4) 的 $a(n)$(参看 §9.6(b) 的定理 9.21).

§9.4 实解析的 Eisenstein 级数

在此我们将引进实解析的 Eisenstein 级数 $E(s,z)$, 并研究它的 Fourier 展开. 其结果不仅限于自守函数论, 而且可以从二次型理论、Laplace 算子理论 (二维环面情形) 等方面进行解释 (按照这种解释, $E(s,z)$ 被称做 Epstein ζ 函数及谱 ζ 函数之类), 它处于现代数学的中心位置. 作为应用我们将给出 Riemann ζ 函数 $\zeta(s)$ 在 $\mathrm{Re}\,(s) = 1$ 上不具零点 (像在 §7.3(a) 所看到的, 这是素数定理证明的关键所在) 的另一个证明.

作为另一个应用, 我们还将叙述 ζ 解析延拓法中的 Rankin–Selberg 方法. 在 §9.5 将可以看到对 Kronecker 极限公式的应用.

(a) $E(s,z)$ 的基本性质

考虑关于上半平面的变量 z 与满足 $\mathrm{Re}(s)>1$ 的复数 s 的级数

$$E(s,z)=\frac{1}{2}\sum_{(c,d)=1}\frac{\mathrm{Im}(z)^s}{|cz+d|^{2s}}$$
$$=\frac{1}{2}y^s\sum_{(c,d)=1}|cz+d|^{-2s}.$$

这是个绝对收敛的级数, 从而是 z 的实解析函数. 我们集中叙述 $E(s,z)$ 的基本性质于下.

定理 9.9

(1) 对于所有的 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$ 成立

$$E\left(s,\frac{az+b}{cz+d}\right)=E(s,z).$$

(2) 具有 Fourier 展开

$$E(s,z)=y^s+\frac{\widehat{\zeta}(2s-1)}{\widehat{\zeta}(2s)}y^{1-s}$$
$$+\frac{4}{\widehat{\zeta}(2s)}\sum_{m=1}^{\infty}m^{s-\frac{1}{2}}\sigma_{1-2s}(m)\sqrt{y}K_{s-\frac{1}{2}}(2\pi my)\cos(2\pi mx).$$

其中,

$$\widehat{\zeta}(s)=\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s),$$
$$\sigma_s(m)=\sum_{d|m}d^s,$$
$$K_s(z)=\frac{1}{2}\int_0^{\infty}\exp\left(-\frac{z}{2}\left(u+\frac{1}{u}\right)\right)u^{s-1}du$$
$$\sim\sqrt{\frac{\pi}{2z}}e^{-z}\quad(z\to+\infty)\quad(\text{变形 Bessel 函数}).$$

特别地, $E(s,z)$ 对于所有 $s\in\mathbb{C}$ 可解析延拓为亚纯函数.

(3) 令 $\widehat{E}(s,z)=\widehat{\zeta}(2s)E(s,z)$, 则其满足函数方程

$$\widehat{E}(s,z)=\widehat{E}(1-s,z).$$

(4) $E(s,z)$ 为上半平面上的 Laplace 算子的特征函数:

$$-y^2(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2})E(s,z)=s(1-s)E(s,z).$$

[证明] (1) 只要对于 $SL_2(\mathbb{Z})$ 的生成元

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

能够证明就可以了. 对 $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ 有

$$E(s,z+1)=\frac{1}{2}\sum_{(c,d)=1}\frac{y^s}{|cz+(c+d)|^{2s}}=E(s,z),$$

而对 $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ 有

$$E(s,-\frac{1}{z})=\frac{1}{2}\sum_{(c,d)=1}\frac{\mathrm{Im}(-\frac{1}{z})^s}{\left|-\frac{c}{z}+d\right|^{2s}},$$

再利用

$$\mathrm{Im}(-\frac{1}{z})=\mathrm{Im}(-\frac{\bar{z}}{z\bar{z}})=-\frac{\mathrm{Im}(\bar{z})}{|z|^2}=\frac{\mathrm{Im}(z)}{|z|^2}$$

便得到

$$E(s,-\frac{1}{z})=\frac{1}{2}\sum_{(c,d)=1}\frac{y^s}{|dz-c|^{2s}}=E(s,z).$$

(4) 只需计算偏微分便知.

(3) 则可利用 (2): 由

$$\begin{aligned}\widehat{E}(s,z)=&\,\widehat{\zeta}(2s)y^s+\widehat{\zeta}(2s-1)y^{1-s}\\&+4\sum_{m=1}^{\infty}m^{s-\frac{1}{2}}\sigma_{1-2s}(m)\sqrt{y}K_{s-\frac{1}{2}}(2\pi my)\cos(2\pi mx),\end{aligned}$$

得到

$$\begin{aligned}\widehat{E}(1-s,z)=&\,\widehat{\zeta}(2-2s)y^{1-s}+\widehat{\zeta}(1-2s)y^s\\&+4\sum_{m=1}^{\infty}m^{\frac{1}{2}-s}\sigma_{2s-1}(m)\sqrt{y}K_{\frac{1}{2}-s}(2\pi my)\cos(2\pi mx).\end{aligned}$$

在其中, 如果使用函数方程 $\widehat{\zeta}(s)=\widehat{\zeta}(1-s)$ 以及

$$① \quad m^{s-\frac{1}{2}}\sigma_{1-2s}(m) = m^{\frac{1}{2}-s}\sigma_{2s-1}(m),$$

$$② \quad K_{s-\frac{1}{2}}(2\pi my) = K_{\frac{1}{2}-s}(2\pi my),$$

则知有 $\widehat{E}(1-s,z) = \widehat{E}(s,z)$. 为了给出 ①, 只要给出更一般的

$$\sigma_t(m) = m^t\sigma_{-t}(m)$$

就行了, 事实上我们有

$$\sigma_t(m) = \sum_{d|m} d^t = \sum_{d|m}\left(\frac{m}{d}\right)^t = m^t\sum_{d|m} d^{-t} = m^t\sigma_{-t}(m).$$

至于 ②, 在

$$K_{-s}(z) = \frac{1}{2}\int_0^\infty \exp\left(-\frac{z}{2}\left(u+\frac{1}{u}\right)\right)u^{-s}\frac{du}{u}$$

中作变量替换 $v = \dfrac{1}{u}$ 则成立

$$K_{-s}(z) = \frac{1}{2}\int_0^\infty \exp\left(-\frac{z}{2}(\frac{1}{v}+v)\right)v^s\frac{dv}{v} = K_s(z).$$

下面证明(2). 其基本的做法是从 $E(s,x+iy)$ 在 $x\to x+1$ 下不变的事实(周期性) 出发, 由于可以展开为 Fourier 级数

$$E(s,z) = \sum_{m=-\infty}^{\infty} a_m(y)e^{2\pi imx},$$

从而只要计算

$$a_m(y) = \int_{-\frac{1}{2}}^{\frac{1}{2}} E(s,x+iy)e^{-2\pi imx}dx$$

就可以了 (参照 §11.2(a)), 这里所使用的积分计算没有太轻松的方法. 我们首先将下式分为两部分:

$$\begin{aligned}\widehat{E}(s,z) &= \pi^{-s}\Gamma(s)\zeta(2s)\cdot\frac{1}{2}\sum_{(c,d)=1}\frac{y^s}{|cz+d|^{2s}}\\ &= \pi^{-s}\Gamma(s)\cdot\frac{1}{2}\sum_{m,n=-\infty}^{\infty}{}'\frac{y^s}{|mz+n|^{2s}}\\ &= \boxed{m=0\text{的项}} + \boxed{m\neq 0\text{ 的项}}.\end{aligned}$$

其中, 对于 m,n 取和处的一撇 “ $'$ ” 表示 $(m,n)\neq(0,0)$. 在此有

$$\begin{aligned}\boxed{m=0\text{的项}} &= \pi^{-s}\Gamma(s)\cdot\frac{1}{2}\sum_{n=-\infty}^{\infty}{}'\frac{y^s}{|n|^{2s}}\\ &= \pi^{-s}\Gamma(s)y^s\sum_{n=1}^{\infty}n^{-2s}\\ &= \pi^{-s}\Gamma(s)y^s\zeta(2s) = \widehat{\zeta}(2s)y^s.\end{aligned}$$

这便求出了第一项(上面对 n 求和处的 "$'$" 表示 $n \neq 0$). 其次, 我们考虑

$$\boxed{m\neq 0 \text{ 的项}} = \pi^{-s}\Gamma(s)\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\frac{y^s}{|mz+n|^{2s}}$$
$$= \pi^{-s}\Gamma(s)y^s\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}((mx+n)^2+m^2y^2)^{-s}.$$

在这里, 对于 $a>0$ 应用

$$\int_0^{\infty} e^{-au}u^s\frac{du}{u} = a^{-s}\Gamma(s)$$

则有

$$\boxed{m\neq 0 \text{ 的项}} = y^s\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\int_0^{\infty} e^{-\pi\{(mx+n)^2+m^2y^2\}u}u^s\frac{du}{u}.$$

进而由 Poisson 求和公式得到的

$$\sum_{n=-\infty}^{\infty} e^{-\pi(mx+n)^2u} = \frac{1}{\sqrt{u}}\sum_{n=-\infty}^{\infty} e^{2\pi imnx}e^{-\frac{\pi n^2}{u}}$$

便知有

$$\boxed{m\neq 0 \text{ 的项}} = y^s\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\left(\int_0^{\infty} e^{-(\pi m^2y^2u+\frac{\pi n^2}{u})}u^{s-\frac{1}{2}}\frac{du}{u}\right)e^{2\pi imnx}$$
$$= y^s\sum_{m=1}^{\infty}\int_0^{\infty} e^{-\pi m^2y^2u}u^{s-\frac{1}{2}}\frac{du}{u}$$
$$+ 2y^s\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\left(\int_0^{\infty} e^{-(\pi m^2y^2u+\frac{\pi n^2}{u})}u^{s-\frac{1}{2}}\frac{du}{u}\right)\cos(2\pi mnx).$$

其中前面的一项为

$$y^s\sum_{m=1}^{\infty}(\pi m^2y^2)^{-(s-\frac{1}{2})}\Gamma\left(s-\frac{1}{2}\right) = y^{1-s}\pi^{-(s-\frac{1}{2})}\Gamma\left(s-\frac{1}{2}\right)\zeta(2s-1)$$
$$= y^{1-s}\widehat{\zeta}(2s-1),$$

而后面的那一项的积分在作了变换 $v=\frac{n}{my}u$ 后成为

$$\int_0^{\infty} e^{-(\pi m^2y^2u+\frac{\pi n^2}{u})}u^{s-\frac{1}{2}}\frac{du}{u} = \int_0^{\infty} e^{-\pi mny(v+\frac{1}{v})}v^{s-\frac{1}{2}}\frac{dv}{v}\cdot\left(\frac{n}{my}\right)^{s-\frac{1}{2}}$$
$$= \left(\frac{n}{my}\right)^{s-\frac{1}{2}}\cdot 2\cdot K_{s-\frac{1}{2}}(2\pi mny).$$

因此,

$$\begin{aligned}
\boxed{m\neq 0 \text{ 的项}} &= \widehat{\zeta}(2s-1)y^{1-s} \\
&\quad + 2y^s\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\left(\frac{n}{my}\right)^{s-\frac{1}{2}}\cdot 2\cdot K_{s-\frac{1}{2}}(2\pi mny)\cos(2\pi mnx) \\
&= \widehat{\zeta}(2s-1)y^{1-s} \\
&\quad + 4\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}m^{1-2s}(mn)^{s-\frac{1}{2}}\sqrt{y}K_{s-\frac{1}{2}}(2\pi mny)\cos(2\pi mnx) \\
&= \widehat{\zeta}(2s-1)y^{1-s} \\
&\quad + 4\sum_{n=1}^{\infty}n^{s-\frac{1}{2}}\sigma_{1-2s}(n)\sqrt{y}K_{s-\frac{1}{2}}(2\pi ny)\cos(2\pi nx).
\end{aligned}$$

在其中的最后一个变换里, mn 被新的 n 所替换. 综合上面的计算得到

$$\begin{aligned}
\widehat{E}(s,z) &= \widehat{\zeta}(2s)y^s + \widehat{\zeta}(2s-1)y^{1-s} \\
&\quad + 4\sum_{m=1}^{\infty}m^{s-\frac{1}{2}}\sigma_{1-2s}(m)\sqrt{y}K_{s-\frac{1}{2}}(2\pi my)\cos(2\pi mx),
\end{aligned}$$

从而得到了 (2). 至于 $E(s,z)$ 可以解析延拓到所有 $s\in\mathbb{C}$ 上, 由各个 Fourier 系数为解析以及从积分表示有 $K_s(y)=O(e^{-y})\ (y\to+\infty)$ 得到 (参照 §11.2(b)). 还有, 当取 (2) 的 Fourier 展开

$$E(s,z)=\sum_{m=-\infty}^{\infty}a_m(y)e^{2\pi imx}$$

时 (此系数可视为 Riemann 猜想的类比) , 记

$$a_m(y)=\begin{cases} y^s+\dfrac{\widehat{\zeta}(2s-1)}{\widehat{\zeta}(2s)}y^{1-s} & m=0 \\ 2|m|^{s-\frac{1}{2}}\sigma_{1-2s}(|m|)\sqrt{y}K_{s-\frac{1}{2}}(2\pi|m|y) & m\neq 0. \end{cases}$$

其中的 $a_0(y)$ 按惯例被称为实解析 Eisenstein 级数的 "常数项"(准确地说, 是相对于 x 的常数项). ∎

(b) 实解析 Eisenstein 级数的应用 (从 $GL(2)$ 到 $GL(1)$)

素数定理 (第七章, 定理 7.5)

$$\pi(x)\sim\frac{x}{\log x}\quad (x\to\infty)$$

的证明关键是

$$\zeta(s)\text{在 } \mathrm{Re}\,(s)\geqslant 1 \text{ 不具有零点}$$

这个重要的事实 (定理 7.3; 证明由 Hadamard 和 de la Vallée-Poussin 在 1896 年给出). 这个事实在与 Riemann 猜想的关联上也是重要的. Riemann 猜想等价于

$$\zeta(s)\text{在 } \mathrm{Re}\,(s) > \frac{1}{2} \text{ 不具有零点}$$

(如果已知 $1 > \mathrm{Re}\,(s) > \frac{1}{2}$ 时无零点, 则由函数方程 $\zeta(s) \leftrightarrow \zeta(1-s)$ 得出在 $0 < \mathrm{Re}\,(s) < \frac{1}{2}$ 时不具有零点). 因此, 对于 $\frac{1}{2} < \alpha < 1$ 可以期望能得到结果

$$\zeta(s)\text{在 } \mathrm{Re}\,(s) \geqslant \alpha \text{ 不具有零点},$$

在 Hadamard 和 de la Vallée-Poussin 之后过了 100 年, 人们仍然不能把他们 $\alpha = 1$ 的结果 (即便是 $\alpha = 0.999999999$) 变成 $\alpha < 1$ 的结果. 按照这个观点, 那么 $\zeta(s)$ 在 $\mathrm{Re}\,(s) \geqslant 1$ 不具有零点的结果中, "1" 是迄今最好的了.

正是由于这样的情况, 如果能给出 $\zeta(s)$ 在 $\mathrm{Re}\,(s) = 1$ 上不具有零点的新证明 ($\mathrm{Re}\,(s) > 1$ 上无零点可立即由 Euler 积得知, 这一部分没有问题), 那么这就是一个非常深刻且有趣的事情. 其中的一个证明便是使用实解析的 Eisenstein 级数给出的.

$\mathrm{Re}\,(s) = 1$ 上 $\zeta(s) \neq 0$ 的另一证明　假设 $\zeta(1+it_0) = 0$ $(t_0 \neq 0)$. 令 $s_0 = \dfrac{1+it_0}{2}$. 在

$$\begin{aligned}\widehat{E}(s_0, z) = &\widehat{\zeta}(2s_0)y^{s_0} + \widehat{\zeta}(2s_0-1)y^{1-s_0}\\ &+ 4\sum_{m=1}^{\infty} m^{s_0-\frac{1}{2}}\sigma_{1-2s_0}(m)\sqrt{y}K_{s_0-\frac{1}{2}}(2\pi my)\cos(2\pi mx)\end{aligned}$$

中

$$\begin{aligned}&\widehat{\zeta}(2s_0) = \widehat{\zeta}(1+it_0) = 0,\\ &\widehat{\zeta}(2s_0-1) = \widehat{\zeta}(it_0) = \widehat{\zeta}(1-it_0) = \overline{\widehat{\zeta}(1+it_0)} = 0.\end{aligned}$$

在这里使用了 $\widehat{\zeta}(s)$ 的函数方程及镜像原理. 因此有

$$\widehat{E}(s_0, z) = 4\sum_{m=1}^{\infty} m^{s_0-\frac{1}{2}}\sigma_{1-2s_0}(m)\sqrt{y}K_{s_0-\frac{1}{2}}(2\pi my)\cos(2\pi mx),$$

由于在 $\widehat{E}(s_0, z)$ 中没有 "常数项"($m = 0$ 的项), 故当 $\mathrm{Im}z \to \infty$ 时它急剧减小.

于是, 有了

$$F(z) = \overline{\widehat{E}(s_0, z)}.$$

那么, $F(z)$ 对于 $\Gamma = SL_2(\mathbb{Z})$ 不变, 且在 $\mathrm{Im}z \to \infty$ 下急剧减小. 现在, 对于 $\mathrm{Re}\,(s) > 1$, 取 $z = x + iy$ 为上半平面的变量, 并考虑

$$\Phi(s) = \int_{-\frac{1}{2}}^{\frac{1}{2}} dx \int_0^{\infty} dy F(z)(\mathrm{Im}z)^{s-2}.$$

这个积分区域为图 9.6 所显示的阴影部分, 它是对于 Γ 的子群

$$\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}$$

的基本区域 $\Gamma_\infty \backslash H$:

$$\Phi(s) = \int_{\Gamma_\infty \backslash H} F(z)(\operatorname{Im} z)^s \frac{dxdy}{y^2}.$$

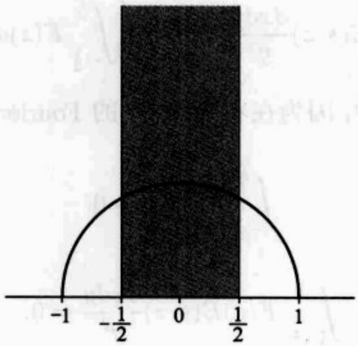


图 9.6

将此基本区域分解为

$$\Gamma_\infty \backslash H = \bigsqcup_{\gamma \in \Gamma_\infty \backslash \Gamma} \gamma(\Gamma \backslash H).$$

其中, γ 遍历 $\Gamma_\infty \backslash \Gamma$ 的完全代表系. 简单的计算表明 $\Gamma_\infty \backslash \Gamma$ 的代表系的元 $\gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix}$ 1-1 对应于 $(c, d) = 1$. 因此, 利用 $\frac{dxdy}{y^2}$ 为 Γ 不变 (进一步说是 $SL_2(\mathbb{R})$ 不变) 的事实, 则有

$$\begin{aligned}
\Phi(s) &= \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \left(\int_{\gamma(\Gamma \backslash H)} F(z)(\operatorname{Im} z)^s \frac{dxdy}{y^2} \right) \\
&= \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \int_{\Gamma \backslash H} F(\gamma z)(\operatorname{Im} \gamma z)^s \frac{dxdy}{y^2} \\
&= \int_{\Gamma \backslash H} F(z) \left(\sum_{\gamma \in \Gamma_\infty \backslash \Gamma} (\operatorname{Im} \gamma z)^s \right) \frac{dxdy}{y^2} \\
&= \int_{\Gamma \backslash H} F(z) E(s, z) \frac{dxdy}{y^2}.
\end{aligned}$$

其中我们用到了对于 $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma$ 有

$$\gamma z=\frac{az+b}{cz+d},$$

从而

$$\mathrm{Im}\gamma z=\frac{\mathrm{Im}z}{|cz+d|^2}.$$

这样, 我们便知等式

$$\int_{\Gamma\backslash H}F(z)E(s,z)\frac{dxdy}{y^2}=\int_0^\infty\left(\int_{-\frac{1}{2}}^{\frac{1}{2}}F(z)dx\right)y^{s-2}dy$$

对于 $\mathrm{Re}\,(s)>1$ 成立. 其中, 因为在右端 $F(z)$ 的 Fourier 展开没有 "常数项", 从而有了

$$\int_{-\frac{1}{2}}^{\frac{1}{2}}F(z)dx=0.$$

因此,

$$\int_{\Gamma\backslash H}F(z)E(s,z)\frac{dxdy}{y^2}=0,$$

进而乘以 $\widehat{\zeta}(2s)$, 于是, 对于 $\mathrm{Re}\,(s)>1$ 成立

$$\int_{\Gamma\backslash H}F(z)\widehat{E}(s,z)\frac{dxdy}{y^2}=0.$$

因此根据解析延拓, 这个等式对于所有的复数 s 都成立. 在此令 $s=s_0$, 那么因为

$$F(z)=\overline{\widehat{E}(s_0,z)},$$

故

$$\int_{\Gamma\backslash H}|F(z)|^2\frac{dxdy}{y^2}=0.$$

因而 $F(z)$ 恒等于 0. 那么 $F(z)$ 的所有的 Fourier 系数应该全为 0, 但是, 譬如第一个 $(m=1)$Fourier 系数

$$K_{s_0-\frac{1}{2}}(2\pi y)=K_{\frac{it_0}{2}}(2\pi y)\sim\frac{1}{2\sqrt{y}}e^{-2\pi y}\quad(y\to+\infty)$$

关于 y 不可能恒等于 0, 从而引出了矛盾. 因此, $\zeta(s)$ 在 $\mathrm{Re}\,(s)=1$ 上不具有零点. ∎

有关方法论的评注

上述证明应用了从 Eisenstein 级数 $E(s,z)$ 这个一般线性群 $GL(2)$ 的自守形式到 Riemann ζ 函数 $\zeta(s)$ 这个 $GL(1)$ 的自守形式 ζ 的转化. Wiles 的 Fermat 大定理

的证明也同样利用了从 $GL(2)$ 到 $GL(1)$ 的转化 (像要在 §12.2 (d) 中叙述的那样, 因利用 $GL(2)$ 的 Sym^2, 有人也应用了从 $GL(3)$ 到 $GL(2)$ 的转化.) 这恰似从二阶看一阶可以很好了解一阶的情形. 至于将 $E(s,z)$ 对 s 进行解析延拓的方法, 在这里除了所使用的 Fourier 系数的解析延拓方法外还有几个证明是由 Selberg 给出的. 按照它们, 反过来则可以知道 Fourier 系数的解析延拓. 例如, 已知

$$\varphi(s) = \frac{\widehat{\zeta}(2s-1)}{\widehat{\zeta}(2s)}$$

为全平面上的亚纯函数. 其中, 在 $\mathrm{Re}\,(s) > \dfrac{1}{2}$ 上分母为绝对收敛从而全纯, 因此再看一看分子就明白了, $\widehat{\zeta}(s)$ 在 $\mathrm{Re}\,(s) > 0$ 为亚纯. 反复如此进行, 则知 $\widehat{\zeta}(s)$ 在 $\mathrm{Re}\,(s) > -1$, $\mathrm{Re}\,(s) > -2, \cdots$ 均为亚纯, 从而在全平面亚纯. 进一步看, 因为按 Selberg 的方法 (Selberg 迹公式的一部分) 得知 $\varphi(s)\varphi(1-s) = 1$, 故而也就知道了 $\widehat{\zeta}(s)$ 的函数方程 (然而, 难于知道它的全纯性). 这样的一些事实也可进一步推广到对于一般群的自守形式的情形. 譬如, 对于 $GL(n)$ 的自守形式的 L 函数的情形, 也可证明 "在 $\mathrm{Re}\,(s) \geqslant 1$ 没有零点" 的事实, 其方法也只是使用了 $GL(n+1)$ 的 Eisenstein 级数而已. (参看第 11 章; 只使用了像定理 7.3 的证明那样的 Euler 积的方法, 而没有用高阶 Euler 积的情形.)

(c) Rankin-Selberg 的方法

自守形式 ζ 的解析延拓方法之一可以应用到 $E(s,z)$ 上. 在 §9.3 中, 我们对 Δ 的自守性进行了 Fourier 变换 (Mellin 变换), 并证明了 $L(s,\Delta)$ 的解析延拓以及函数方程, 在这里, 用

$$\begin{aligned} L(s,\Delta) &= \prod_p (1-\tau(p)p^{-s}+p^{11-2s})^{-1} \\ &= \prod_p [(1-\alpha_p p^{-s})(1-\beta_p p^{-s})]^{-1} \end{aligned}$$

由张量积构造出两类的 4 次 Euler 积:

$$\begin{aligned} L(s,\Delta\otimes\Delta) &= \prod_p [(1-\alpha_p^2 p^{-s})(1-\alpha_p\beta_p p^{-s})(1-\beta_p\alpha_p p^{-s})(1-\beta_p^2 p^{-s})]^{-1} \\ &= \zeta(s-11)L(s,\mathrm{Sym}^2\Delta) \end{aligned}$$

以及

$$\begin{aligned} L(s,\Delta\otimes E_{12}) &= \prod_p [(1-\alpha_p p^{-s})(1-\alpha_p p^{11}p^{-s})(1-\beta_p p^{-s})(1-\beta_p p^{11}p^{-s})]^{-1} \\ &= L(s,\Delta)L(s-11,\Delta), \end{aligned}$$

我们来证明它们的解析延拓并给出函数方程(稍许一般化). 留意一下, 这样, 后一个方程便可给出 $L(s,\Delta)$ 解析延拓的另一个证明. 这里用的方法是在 1939 年左右由

Rankin 和 Selberg 所发现的, 称之为**Rankin-Selberg 方法**, 可以使用它来做各种各样的推广.

定理 9.10 (Rankin-Selberg)

已知

$$f(z)=\sum_{n=1}^{\infty}a(n)q^n,$$
$$g(z)=\sum_{n=1}^{\infty}b(n)q^n,$$

设对于整数 $k>0$ 满足下面的条件(i), (ii):

(i) 对于所有的 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma=SL_2(\mathbb{Z})$ 有

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)^k f(z),$$
$$g\left(\frac{az+b}{cz+d}\right)=(cz+d)^k g(z).$$

(ii) $a(1)=b(1)=1$, 而 $a(n),b(n)$ 为被某个常数 C 的 $O(n^C)$ 所控制的实数, 并令

$$L(s,f)=\sum_{n=1}^{\infty}a(n)n^{-s},$$
$$L(s,g)=\sum_{n=1}^{\infty}b(n)n^{-s}$$

以及

$$\begin{aligned}L(s,f)&=\prod_p(1-a(p)p^{-s}+p^{k-1-2s})^{-1}\\&=\prod_p[(1-\alpha_1(p)p^{-s})(1-\alpha_2(p)p^{-s})]^{-1}\\L(s,g)&=\prod_p(1-b(p)p^{-s}+p^{k-1-2s})^{-1}\\&=\prod_p[(1-\beta_1(p)p^{-s})(1-\beta_2(p)p^{-s})]^{-1}.\end{aligned}$$

这时, 令

$$\begin{aligned}L(s,f\otimes g)=\prod_p&[(1-\alpha_1(p)\beta_1(p)p^{-s})(1-\alpha_1(p)\beta_2(p)p^{-s})\\&\times(1-\alpha_2(p)\beta_1(p)p^{-s})(1-\alpha_2(p)\beta_2(p)p^{-s})]^{-1},\end{aligned}$$

则成立

(1) $L(s,f\otimes g)=\zeta(2s-2k+2)\sum_{n=1}^{\infty}a(n)b(n)n^{-s}$.

(2) $L(s,f\otimes g)$ 可解析延拓为全 s 平面上的亚纯函数, 且

$$\widehat{L}(s,f\otimes g)=\Gamma_{\mathbb{C}}(s)\Gamma_{\mathbb{C}}(s-k+1)L(s,f\otimes g)$$

满足函数方程

$$\widehat{L}(s,f\otimes g)=\widehat{L}(2k-1-s,f\otimes g),$$

其中 $\Gamma_{\mathbb{C}}(s)=2(2\pi)^{-s}\Gamma(s)$.

[证明] 证明 (1). 因为由条件 (ii) 得知 $a(n),b(n)$ 为乘性函数, 故有

$$\sum_{n=1}^{\infty}a(n)b(n)n^{-s}=\prod_{p}\left(\sum_{l=0}^{\infty}a(p^l)b(p^l)p^{-ls}\right).$$

进而, 根据条件 (ii) 有

$$\begin{aligned}\sum_{l=0}^{\infty}a(p^l)u^l&=\frac{1}{1-a(p)u+p^{k-1}u^2}\\&=\frac{1}{(1-\alpha_1(p)u)(1-\alpha_2(p)u)}\\&=(1+\alpha_1(p)u+\alpha_1(p)^2u^2+\cdots)(1+\alpha_2u+\alpha_2(p)^2u^2+\cdots),\end{aligned}$$

于是得到

$$\begin{aligned}a(p^l)&=\alpha_1(p)^l+\alpha_1(p)^{l-1}\alpha_2(p)+\cdots+\alpha_1(p)\alpha_2(p)^{l-1}+\alpha_2(p)^l\\&=\frac{\alpha_1(p)^{l+1}-\alpha_2(p)^{l+1}}{\alpha_1(p)-\alpha_2(p)}\end{aligned}$$

(当 $\alpha_1(p)=\alpha_2(p)$ 时, 可以更简单地计算). 同样有

$$b(p^l)=\frac{\beta_1(p)^{l+1}-\beta_2(p)^{l+1}}{\beta_1(p)-\beta_2(p)},$$

计算幂级数有

$$\begin{aligned}&\sum_{l=0}^{\infty}a(p^l)b(p^l)u^l\\&=\sum_{l=0}^{\infty}\left(\frac{\alpha_1(p)^{l+1}-\alpha_2(p)^{l+1}}{\alpha_1(p)-\alpha_2(p)}\right)\left(\frac{\beta_1(p)^{l+1}-\beta_2(p)^{l+1}}{\beta_1(p)-\beta_2(p)}\right)u^l\\&=\frac{1}{(\alpha_1(p)-\alpha_2(p))(\beta_1(p)-\beta_2(p))}\left\{\frac{\alpha_1(p)\beta_1(p)}{1-\alpha_1(p)\beta_1(p)u}\right.\\&\quad\left.+\frac{\alpha_2(p)\beta_2(p)}{1-\alpha_2(p)\beta_2(p)u}-\frac{\alpha_1(p)\beta_2(p)}{1-\alpha_1(p)\beta_2(p)u}-\frac{\alpha_2(p)\beta_1(p)}{1-\alpha_2(p)\beta_1(p)u}\right\}\\&=\frac{1-\alpha_1(p)\alpha_2(p)\beta_1(p)\beta_2(p)u^2}{(1-\alpha_1(p)\beta_1(p)u)(1-\alpha_1(p)\beta_2(p)u)(1-\alpha_2(p)\beta_1(p)u)(1-\alpha_2(p)\beta_2(p)u)},\end{aligned}$$

因为

$$\alpha_1(p)\alpha_2(p)\beta_1(p)\beta_2(p) = p^{2k-2}$$

故知 (1) 成立.

下面证明 (2). 首先我们注意到, 由于

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} f(z)\overline{g(z)}dx = \sum_{n,m=1}^{\infty} a(n)b(m)\left(\int_{-\frac{1}{2}}^{\frac{1}{2}} e^{2\pi i(n-m)x}dx\right)e^{-2\pi(n+m)y}$$
$$= \sum_{n=1}^{\infty} a(n)b(n)e^{-4\pi ny}$$

故而有

$$\int_0^{\infty}\left(\int_{-\frac{1}{2}}^{\frac{1}{2}} f(z)\overline{g(z)}dx\right)y^{s-1}dy = (4\pi)^{-s}\Gamma(s)\sum_{n=1}^{\infty} a(n)b(n)n^{-s}$$
$$\underset{(1)}{=} (4\pi)^{-s}\Gamma(s)\frac{L(s, f\otimes g)}{\zeta(2s-2k+2)}.$$

由此以类似于 §9.4(b) 的方法, 并使用那里的记号, 则有

$$\begin{aligned}
&(4\pi)^{-s}\Gamma(s)L(s, f\otimes g)\\
&= \zeta(2s-2k+2)\int_0^{\infty}\left(\int_{-\frac{1}{2}}^{\frac{1}{2}} f(z)\overline{g(z)}dx\right)y^{s-1}dy\\
&= \zeta(2s-2k+2)\int_{\Gamma_\infty\backslash H} f(z)\overline{g(z)}y^{s+1}\frac{dxdy}{y^2}\\
&= \zeta(2s-2k+2)\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\left(\int_{\gamma(\Gamma\backslash H)}(f(z)\overline{g(z)}y^k)y^{s-k+1}\frac{dxdy}{y^2}\right)\\
&= \zeta(2s-2k+2)\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\left(\int_{\Gamma\backslash H}(f(z)\overline{g(z)}y^k)(\mathrm{Im}\gamma z)^{s-k+1}\frac{dxdy}{y^2}\right)\\
&= \zeta(2s-2k+2)\int_{\Gamma\backslash H} f(z)\overline{g(z)}y^k\left(\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}(\mathrm{Im}\gamma z)^{s-k+1}\right)\frac{dxdy}{y^2}\\
&= \zeta(2s-2k+2)\int_{\Gamma\backslash H} f(z)\overline{g(z)}y^k E(s-k+1, z)\frac{dxdy}{y^2}.
\end{aligned}$$

其中用到了 $f(z)\overline{g(z)}y^k$ 根据条件 (i) 为 Γ 不变的性质. 如此得到的这个积分号内部, 是 s 的亚纯函数, 故考察此积分收敛性得知 $L(s, f\otimes g)$ 是个亚纯函数. 函数方程则由

$$\widehat{L}(f\otimes g) = 2^{k+1}\int_{\Gamma\backslash H} f(z)\overline{g(z)}y^k\widehat{E}(s-k+1, z)\frac{dxdy}{y^2}$$

得到. ∎

在这个定理中令

$$g = -\frac{B_k}{2k}E_k$$
$$= -\frac{B_k}{2k} + \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

(乘以常数倍并不怎么重要), 由于 $\sigma_{k-1}(n)$ 是乘性的, 故有

$$L(s,g) = \sum_{n=1}^{\infty}\sigma_{k-1}(n)n^{-s} = \prod_p\left(\sum_{l=0}^{\infty}\sigma_{k-1}(p^l)p^{-ls}\right),$$

再由

$$\sigma_{k-1}(p^l) = 1 + p^{k-1} + \cdots + (p^l)^{k-1} = \frac{1-p^{(l+1)(k-1)}}{1-p^{k-1}}$$

而得到

$$\sum_{l=0}^{\infty}\sigma_{k-1}(p^l)u^l = \frac{1}{(1-u)(1-p^{k-1}u)},$$

从而

$$L(s,g) = \zeta(s)\zeta(s-k+1),$$

故知

$$L(s,f\otimes g) = L(s,f)L(s-k+1,f).$$

因此也得出了 $L(s,f)$ 以及 $L(s,\Delta)$ 的解析延拓 (这可看作 "从 $GL(4)$ 到 $GL(2)$ 的应用"). 函数方程的形式也与定理 9.7 相一致.

再有, Rankin(1939 年) 将该定理用于

$$L(s,\Delta\otimes\Delta) = \zeta(2s-22)\sum_{n=1}^{\infty}\tau(n)^2 n^{-s},$$

并仔细地查看在 $s=12$ 具有一阶极点的情形, 而得到了估值

$$\tau(n) = O(n^{\frac{29}{5}}).$$

这对于在定理 9.7 处所写下的估值

$$\tau(n) = O(n^6)$$

中的 6 改进了 (小小的)$\frac{1}{5}$. 这是个朝着 Ramanujan 猜想 (等价于 $\tau(n) = O(n^{\frac{11}{2}+\varepsilon})$; 参看习题 9.5) 的方向前进了一步的结果. Deligne 所给出的对于 Ramanujan 猜想的证明设想便得益于 Rankin 的这一方法的启示, 简单地说, 即只要考虑对于不断增大 m 的级数

$$\sum_{n=1}^{\infty}\tau(n)^m n^{-s}$$

就可以了 (Deligne 的方法比起代数几何方式以更容易处理的形式对其进行了阐述).

§9.5 Kronecker 极限公式与正规积

在 (a)—(c) 小节中我们将对 Kronecker 极限公式和正规积给予系统阐述, 其应用则放在 (d)—(f) 中叙述.

(a) Kronecker 极限公式

定理 9.11 (Kronecker 极限公式)

$$\frac{\partial}{\partial s}E(0,z)=\frac{1}{6}\log(y^6|\Delta(z)|).$$

[证明] 对于

$$E(s,z)=y^s+\frac{\pi^{s-1}\Gamma(1-s)\zeta(2-2s)}{\pi^{-s}\Gamma(s)\zeta(2s)}y^{1-s}$$
$$+\frac{4}{\pi^{-s}\Gamma(s)\zeta(2s)}\sum_{m=1}^{\infty}m^{s-\frac{1}{2}}\sigma_{1-2s}(m)\sqrt{y}K_{s-\frac{1}{2}}(2\pi my)\cos(2\pi mx),$$

应用在 $s=0$ 的 Taylor 展开

$$\frac{\pi^{s-1}\Gamma(1-s)\zeta(2-2s)}{\pi^{-s}\Gamma(s)\zeta(2s)}=\pi^{-1}\frac{\zeta(2)}{\zeta(0)}s+[s\text{的大于等于 2 次的项}],$$
$$\frac{4}{\pi^{-s}\Gamma(s)\zeta(2s)}=\frac{4}{\zeta(0)}s+[s\text{的大于等于 2 次的项}],$$

于是有

$$E(0,z)=1$$

及

$$\frac{\partial}{\partial s}E(0,z)=\log y+\frac{\pi^{-1}\zeta(2)}{\zeta(0)}y$$
$$+\frac{4}{\zeta(0)}\sum_{m=1}^{\infty}m^{-\frac{1}{2}}\sigma_1(m)\sqrt{y}K_{\frac{1}{2}}(2\pi my)\cos(2\pi mx).$$

其中的 $\sigma_1(m)=\sum\limits_{d|m}d$ 只简单地以 $\sigma(m)$ 记之, 而

$$K_{\frac{1}{2}}(z)=\sqrt{\frac{\pi}{2z}}e^{-z}$$

(Euler 的计算). 实际上, 在

$$K_{\frac{1}{2}}(z)=\frac{1}{2}\int_0^{\infty}\exp\left(-\frac{z}{2}\left(u+\frac{1}{u}\right)\right)u^{-\frac{1}{2}}\frac{du}{u}$$

中, 作变换 $v=\frac{z}{2}u$, 则有

$$K_{\frac{1}{2}}(z)=\frac{1}{\sqrt{2z}}\int_0^{\infty}\exp\left(-\left(v+\frac{z^2}{4v}\right)\right)v^{\frac{1}{2}}\frac{dv}{v}.$$

因此在

$$\frac{d}{dz}\left(\sqrt{2z}K_{\frac{1}{2}}(z)\right) = -\frac{z}{2}\int_0^\infty \exp\left(-\left(v+\frac{z^2}{4v}\right)\right)v^{-\frac{1}{2}}\frac{dv}{v}$$

中作替换 $w = \frac{z^2}{4v}$, 则有

$$\begin{aligned}\frac{d}{dz}\left(\sqrt{2z}K_{\frac{1}{2}}(z)\right) &= -\int_0^\infty \exp\left(-\left(w+\frac{z^2}{4w}\right)\right)w^{-\frac{1}{2}}\frac{dw}{w}\\ &= -\left(\sqrt{2z}K_{\frac{1}{2}}(z)\right).\end{aligned}$$

由此得知

$$\begin{aligned}\sqrt{2z}K_{\frac{1}{2}}(z) &= Ce^{-z},\\ C &= \int_0^\infty e^{-v}v^{-\frac{1}{2}}dv = \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}.\end{aligned}$$

于是, 便有

$$\frac{\partial}{\partial s}E(0,z) = \log y - \frac{\pi}{3}y - 4\sum_{m=1}^{\infty}\frac{\sigma(m)}{m}e^{-2\pi my}\cos(2\pi mx).$$

另一方面, 由于

$$\begin{aligned}\log(y^6|\Delta(z)|) &= 6\log y + \log|\Delta(z)|\\ &= 6\log y + \mathrm{Re}\,(\log\Delta(z))\\ &= 6\log y - 2\pi y - 24\cdot\mathrm{Re}\left(\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{1}{m}q^{nm}\right)\\ &= 6\log y - 2\pi y - 24\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{1}{m}e^{-2\pi mny}\cos(2\pi mnx)\\ &= 6\log y - 2\pi y - 24\sum_{m=1}^{\infty}\frac{\sigma(m)}{m}e^{-2\pi my}\cos(2\pi mx),\end{aligned}$$

故而得到了所要的等式. ∎

这里的 "Kronecker 极限公式" 与原叙述

$$\lim_{s\to 1}(\zeta(2s)E(s,z) - \frac{\pi}{2}\cdot\frac{1}{s-1}) = \pi\left\{\gamma - \log 2 - \log\left(y^{\frac{1}{2}}|\Delta(z)|^{\frac{1}{12}}\right)\right\}$$

的形式不同. 原式中的

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right) = 0.577\cdots$$

为 Euler 常数. 由函数方程 $\widehat{E}(1-s,z)=\widehat{E}(s,z)$ 知, 此结果与上面的定理是等价的. 但一般地总是以在 $s=0$ 的微分的形式来简明地表示.

(b) 正规积

对于数列 $\boldsymbol{a}=(a_1,a_2,a_3,\cdots)$, 取其 ζ 为

$$\zeta_{\boldsymbol{a}}(s)=\sum_{n=1}^{\infty}a_n^{-s},$$

当它在 $s=0$ 的邻域可解析延拓为全纯函数时, 则定义 $a_1,a_2,a_3,\cdots$ 的**正规积** (normalized product) 为

$$\prod_{n=1}^{\infty}a_n=\exp(-\zeta_{\boldsymbol{a}}'(0)).$$

这一定义的想法是: 在有限数列 $\boldsymbol{a}=(a_1,\cdots,a_N)$ 时, 由

$$\zeta_{\boldsymbol{a}}(s)=\sum_{n=1}^{N}a_n^{-s}$$

得到

$$\zeta_{\boldsymbol{a}}'(0)=-\sum_{n=1}^{N}\log(a_n)=-\log\left(\prod_{n=1}^{N}a_n\right).$$

因此便有

$$\exp(-\zeta_{\boldsymbol{a}}'(0))=\prod_{n=1}^{N}a_n.$$

在无限的情形取正规积会得到许多超出想象的有较深刻意义的东西. 在其后我们可以看到其中的几个, 而这样无限积的最初的例子是由 Riemann (1859年) 给出的

$$\prod_{n=1}^{\infty}n=\sqrt{2\pi}.$$

这由 $\boldsymbol{a}=(1,2,3,\cdots)$ 的 $\zeta_{\boldsymbol{a}}(s)$ 为 Riemann ζ 函数

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s},$$

所要求的值正是

$$\zeta'(0)=-\frac{1}{2}\log(2\pi)$$

而得到. Riemann 在这个计算中使用了 $\zeta(s)$ 的函数方程 (参照 §7.3(d)), 在此我们将给出由 Lerch(1894年) 在更一般情形下的证明. 回忆 Hurwitz ζ 的定义:

$$\zeta(s,x)=\sum_{n=0}^{\infty}(n+x)^{-s}.$$

它在 $\mathrm{Re}\,(s)>1$ 时绝对收敛, 并可解析延拓为整个 s 平面的亚纯函数 (参照 §3.3).

定理 9.12 (Lerch 公式)

$$\prod_{n=0}^{\infty}(n+x)=\frac{\sqrt{2\pi}}{\Gamma(x)}$$

即

$$\frac{\partial}{\partial s}\zeta(0,x)=\log\frac{\Gamma(x)}{\sqrt{2\pi}}.$$

[证明] 令

$$f(x)=\frac{\partial}{\partial s}\zeta(0,x)-\log\Gamma(x).$$

我们按下面的顺序来证明

$$f(x)=-\frac{1}{2}\log(2\pi):$$

(i) $f''(x)=0$. 从而可写 $f(x)=ax+b$.

(ii) $f(x+1)=f(x)$. 从而 $f(x)=b$.

(iii) $f\left(\frac{1}{2}\right)=-\frac{1}{2}\log(2\pi)$. 从而 $f(x)=-\frac{1}{2}\log(2\pi)$.

证明 (i). 我们注意到有

$$f''(x)=\frac{\partial^3}{\partial x^2\partial s}\zeta(0,x)-\frac{d^2}{dx^2}\log\Gamma(x).$$

首先, 由

$$\zeta(s,x)=\sum_{n=0}^{\infty}(n+x)^{-s}\qquad(\mathrm{Re}\,(s)>1)$$

有

$$\frac{\partial^2}{\partial x^2}\zeta(s,x)=\sum_{n=0}^{\infty}s(s+1)(n+x)^{-s-2},$$

故

$$\frac{\partial^3}{\partial s\partial x^2}\zeta(0,x)=\sum_{n=0}^{\infty}(n+x)^{-2}.$$

另一方面, 由 Γ 函数的积表达式

$$\frac{1}{\Gamma(x)}=xe^{\gamma x}\prod_{n=1}^{\infty}\left(1+\frac{x}{n}\right)e^{-\frac{x}{n}}$$

($\gamma=0.577\cdots$ 为 Euler 常数) 有

$$-\log\Gamma(x)=\log x+\gamma x+\sum_{n=1}^{\infty}\left(\log\left(1+\frac{x}{n}\right)-\frac{x}{n}\right),$$

于是得知

$$-\frac{d^2}{dx^2}\log\Gamma(x)=-\frac{1}{x^2}-\sum_{n=1}^{\infty}\frac{1}{(n+x)^2}=-\sum_{n=0}^{\infty}(n+x)^{-2}.$$

因此得到 $f''(x)=0$.

证明 (ii). 由

$$\zeta(s,x+1)=\sum_{n=0}^{\infty}(n+(x+1))^{-s}=\sum_{n=0}^{\infty}((n+1)+x)^{-s}=\zeta(s,x)-x^{-s}$$

有

$$\frac{\partial}{\partial s}\zeta(0,x+1)=\frac{\partial}{\partial s}\zeta(0,x)+\log x.$$

另一方面,

$$\Gamma(x+1)=x\Gamma(x),$$

故

$$\log\Gamma(x+1)=\log\Gamma(x)+\log x.$$

因此得到 $f(x+1)=f(x)$.

再证明 (iii). 我们来计算

$$f\left(\frac{1}{2}\right)=\frac{\partial}{\partial s}\zeta\left(0,\frac{1}{2}\right)-\log\Gamma\left(\frac{1}{2}\right).$$

由

$$\zeta\left(s,\frac{1}{2}\right)=\sum_{n=0}^{\infty}\left(n+\frac{1}{2}\right)^{-s}=2^{s}\sum_{n=0}^{\infty}(2n+1)^{-s}=(2^{s}-1)\zeta(s)$$

得到

$$\frac{\partial}{\partial s}\zeta\left(0,\frac{1}{2}\right)=(\log 2)\zeta(0)=-\frac{1}{2}\log 2.$$

再利用

$$\begin{aligned}\Gamma\left(\frac{1}{2}\right)&=\int_0^{\infty}e^{-u}u^{-\frac{1}{2}}du \qquad (u=x^2)\\&=2\int_0^{\infty}e^{-x^2}dx=\sqrt{\pi},\end{aligned}$$

最后得到了 $f\left(\frac{1}{2}\right)=-\frac{1}{2}\log(2\pi)$. ∎

推论 9.13 (Riemann)

$$\prod_{n=1}^{\infty}n=\sqrt{2\pi}.$$

[证明] 在定理 9.12 中令 $x=1$ 即可. (这个结果可解释为 "$\infty!$" $=\sqrt{2\pi}$.) ∎

那么, Kronecher 极限公式 (定理 9.11) 若使用正规积则可改写为下面的形式.

定理 9.14 (Kronecker 极限公式)

(1) $\prod_{(c,d)=1} \frac{|cz+d|}{\sqrt{y}} = (y^6|\Delta(z)|)^{-\frac{1}{6}}$.

(2) $\prod_{m,n=-\infty}^{\infty}{}' \frac{|mz+n|}{\sqrt{y}} = 2\pi(y^6|\Delta(z)|)^{\frac{1}{12}}$.

[证明] 证明 (1). 令

$$\varphi_1(s) = \sum_{(c,d)=1} \left(\frac{|cz+d|}{\sqrt{y}}\right)^{-s}$$

则有

$$\varphi_1(s) = 2E\left(\frac{s}{2}, z\right),$$

故而有

$$\varphi_1'(0) = \frac{\partial}{\partial s}E(0,z) = \frac{1}{6}\log\left(y^6|\Delta(z)|\right).$$

下面证明 (2). 令

$$\varphi_2(s) = \sum_{m,n=-\infty}^{\infty} \left(\frac{|mz+n|}{\sqrt{y}}\right)^{-s},$$

则有

$$\varphi_2(s) = 2\zeta(s)E\left(\frac{s}{2}, z\right),$$

故

$$\varphi_2'(0) = -\frac{1}{2}\frac{\partial}{\partial s}E(0,z) - \log(2\pi)\cdot E(0,z),$$

那么利用 $E(0,z)=1$ 以及

$$\frac{\partial}{\partial s}E(0,z) = \frac{1}{6}\log(y^6|\Delta(z)|)$$

就得到了证明. ∎

正规积不存在的例子

正规积 $\prod_{n=1}^{\infty} a_n$ 不一定存在.

① $a_n = 2^n \quad (n=1,2,\cdots)$:

此时,

$$\zeta_a(s) = \sum_{n=1}^{\infty} 2^{-ns} = \frac{1}{2^s-1},$$

它以 $s=0$ 为极点. 因此 $\prod_{n=1}^{\infty} 2^n$ 不存在.

② $a_n = p_n \ (n=1,2,\cdots)$ 为第 n 个素数:

此时

$$\zeta_a(s) = \sum_{n=1}^{\infty} p_n^{-s}$$

为在 $\mathrm{Re}\,(s) > 0$ 上的解析函数 (具有不一定是极点的奇点), 并且 $\mathrm{Re}\,(s) = 0$ 为其自然边界 (Laudau-Walfisz, 1919年). 特别地, $s = 0$ 是个本性奇点. 因此 $\prod\limits_{n=1}^{\infty} p_n$ 不存在.

(c) 行列式表示

Lerch 公式也可解释为行列式表示:

$$\prod_{n=0}^{\infty}(n+x) = \mathrm{Det}(D+x) = \frac{\sqrt{2\pi}}{\Gamma(x)}.$$

其中

$$D = t\frac{d}{dt} : \mathbb{C}[t] \to \mathbb{C}[t].$$

此时 D 的特征值为 $n = 0, 1, 2, \cdots$, 而相应的特征函数为 t^n ($Dt^n = nt^n$). 另外, 行列式 Det 是"正规行列式", 即对于矩阵 A (算子) 的行列, 定义

$$\mathrm{Det}A = \prod_{\lambda:A\text{的特征值}} \lambda.$$

因此, 像在第七章所见 (按照阿代尔的观点) Γ 函数是 ζ 的 "无限分量", 那么考虑 ζ 的中间分量是很自然的. 进一步说, 在 $\Gamma(s)$ 情形的 "Riemann 猜想类比" 可考虑为 "$\Gamma(s)$ 的极点全在实轴 $\mathrm{Im}(s) = 0$ 上". 这样来看的话, Lerch 公式便是说 "ζ 是一个适当的算子的行列式 ('特征多项式')":

$$\boxed{\text{Zet}} = \boxed{\text{Det}}$$

这可以看作一个一般性猜想中的一个环节, 这是在 1915 年由 Hilbert 和 Pólya 提出的关于 Riemann ζ 的一个猜想. 已被确认了有这样的行列式表示的 ζ 有

(1) 同余 ζ: 有限域上的代数簇的 ζ (参看 §7.4),

(2) Selberg ζ: Riemann 流形的 ζ (参看第十一章),

(3) p 进 ζ (p 进 L 函数): 相当于岩泽主猜想 (参看第十章) 等等,

它们显示出了各种各样非常重要的事实. 特别地, 在 (1) 与 (2) 的情形中, 由这些行列式表示可以将 ζ 的极点和零点解释为特征值, 其结果推导出了类比的 Riemann 猜想成立.

还有, 在 (1) 与 (2) 中出现的算子是 Frobenius 算子 (的对数) 和 Laplace 算子 (的平方根), 它们在各自的理论中起着中心的作用. 在 (3) 中应该也会出现所说的 "岩泽算子"(参看 §10.0(e)). 这样一来, ζ 的行列式表示便表现为理论的核心了. 行列式表示所留下的 ζ 为 Riemann ζ, 以及 Dedkind ζ 等等原本都是数论的 ζ, 还有待将

它们解释清楚.

(d) Δ 的变换公式

Kronecker 的极限公式 (定理 9.14) 可以用来证明 $\Delta(z)$ 的变换公式. 这是在 §9.2 的定理 9.4 中作为方法 (2) 所叙述的. 我们来进行一点补充. 在定理 9.14 里, 令 $z = iy$ 则

$$\prod_{m,n=-\infty}^{\infty}{}' \sqrt{\frac{m^2y^2+n^2}{y}} = 2\pi y^{\frac{1}{2}}\Delta(iy)^{\frac{1}{12}},$$

因此有

$$2\pi\left(\frac{1}{y}\right)^{\frac{1}{2}}\Delta\left(i\frac{1}{y}\right)^{\frac{1}{12}} = \prod_{m,n=-\infty}^{\infty}{}' \sqrt{\frac{m^2\dfrac{1}{y^2}+n^2}{\dfrac{1}{y}}} = \prod_{m,n=-\infty}^{\infty}{}' \sqrt{\frac{n^2y^2+m^2}{y}},$$

从而得知

$$2\pi y^{\frac{1}{2}}\Delta(iy)^{\frac{1}{12}} = 2\pi\left(\frac{1}{y}\right)^{\frac{1}{2}}\Delta\left(i\frac{1}{y}\right)^{\frac{1}{12}}.$$

于是有了

$$\Delta\left(i\frac{1}{y}\right) = y^{12}\Delta(iy).$$

这样便知道 $\Delta\left(-\frac{1}{z}\right) = z^{12}\Delta(z)$, 从而得出 $\Delta(z)$ 的变换公式.

(e) E_2 的变换公式

令

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma(n)q^n.$$

这里, $\sigma(n) = \sigma_1(n) = \sum\limits_{d|n} d$. 它具有 “权 2 的 Eisenstein 级数” 的性质. 然而, 像在 §9.6 将要证明的那样, 在 $SL_2(\mathbb{Z})$ 的情形, 权 2 的全纯自守形式只有 0, 确切的意思是说, 不存在权 2 的 Eisenstein 级数.

定理 9.15

(1) $E_2\left(-\frac{1}{z}\right) = z^2E_2(z) + \frac{6z}{\pi i}$.

(2) $E_2(i) = \frac{3}{\pi}$.

(3) $\sum\limits_{n=1}^{\infty}\frac{n}{e^{2\pi n}-1} = \frac{1}{24} - \frac{1}{8\pi}$.

[证明]　(1) 对 $\Delta\left(-\frac{1}{z}\right) = z^{12}\Delta(z)$ 两端取对数微分. 因

$$\log\left(\Delta\left(-\frac{1}{z}\right)\right) = -\frac{2\pi i}{z} - 24\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{-\frac{2\pi i n}{z}},$$

故有

$$\frac{1}{2\pi i}\frac{d}{dz}\log\left(\Delta\left(-\frac{1}{z}\right)\right) = \frac{1}{z^2} - 24\frac{1}{z^2}\sum_{n=1}^{\infty}\sigma(n)e^{-\frac{2\pi i n}{z}}.$$

另一方面, 由于

$$\log(z^{12}\Delta(z)) = 12\log z + 2\pi i z - 24\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi i n z}$$

故

$$\frac{1}{2\pi i}\frac{d}{dz}\log(z^{12}\Delta(z)) = \frac{6}{\pi i z} + 1 - 24\sum_{n=1}^{\infty}\sigma(n)e^{2\pi i n z}.$$

因此,

$$\frac{1}{z^2} - 24\frac{1}{z^2}\sum_{n=1}^{\infty}\sigma(n)e^{-\frac{2\pi i n}{z}} = \frac{6}{\pi i z} + 1 - 24\sum_{n=1}^{\infty}\sigma(n)e^{2\pi i n z}.$$

这恰好就是

$$\frac{1}{z^2}E_2(-\frac{1}{z}) = \frac{6}{\pi i z} + E_2(z).$$

(2) 在 (1) 中若令 $z = i$, 则

$$E_2(i) = -E_2(i) + \frac{6}{\pi}.$$

因此

$$E_2(i) = \frac{3}{\pi}.$$

(3) 根据 (2), 有

$$\sum_{n=1}^{\infty}\sigma(n)e^{-2\pi n} = \frac{1}{24} - \frac{1}{8\pi},$$

将左端以 Lambert 级数改写, 则为

$$\sum_{n=1}^{\infty}\frac{n}{e^{2\pi n} - 1}.$$ ■

注记　因为由 (1) 的证明有

$$\frac{1}{2\pi i}\frac{\Delta'}{\Delta}(z) = \frac{1}{2\pi i}\frac{d}{dz}(\log\Delta)(z) = 1 - 24\sum_{n=1}^{\infty}\sigma(n)q^n = E_2(z),$$

若能够直接证明

$$E_2(-\frac{1}{z}) = z^2 E_2(z) + \frac{6z}{\pi i},$$

则可反过来推导出 Δ 的变换公式: 因为

$$\begin{aligned}\frac{d}{dz}\log\left(\Delta\left(-\frac{1}{z}\right)\Big/\Delta(z)\right) &= \frac{1}{z^2}\frac{\Delta'}{\Delta}\left(-\frac{1}{z}\right) - \frac{\Delta'}{\Delta}(z)\\ &= \frac{2\pi i}{z^2}E_2\left(-\frac{1}{z}\right) - 2\pi i E_2(z)\\ &= \frac{2\pi i}{z^2}\left(E_2\left(-\frac{1}{z}\right) - z^2 E_2(z)\right)\\ &= \frac{2\pi i}{z^2}\cdot\frac{6z}{\pi i} = \frac{12}{z},\end{aligned}$$

从而存在常数 C 使得

$$\Delta(-\frac{1}{z}) = \Delta(z)Cz^{12},$$

令 $z = i$ 得到 $C = 1$. $E_2(z)$ 的变换公式的 "直接证明" 是 Hurwitz (1904年) 利用了条件收敛级数

$$E_2(z) = \sum_{n=-\infty}^{\infty}\left(\sum_{m=-\infty}^{\infty}\frac{1}{(mz+n)^2}\right) \qquad ((m,n)\neq(0,0))$$

给出的 (参照 J.-P. Serre 的《A Course in arithmetic》, GTM 7). 再有, 对 $E_2(z)$ 关于 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ 的变换公式

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z)$$

取对数微分得到

$$E_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 E_2(z) + \frac{6c(cz+d)}{\pi i}.$$

(f) $\Delta(i)$ 与 $E_4(i)$ 的计算

令

$$\varpi = 2\int_0^1 \frac{dr}{\sqrt{1-r^4}} = 2.62205\cdots.$$

这是双纽线 $x^2+y^2=\sqrt{x^2-y^2}$ 的半周长: 在极坐标表示 $r^2=\cos(2\theta)$ 下计算即可 (图 9.7). 使用 Γ 函数则有

$$\varpi = 2^{-\frac{3}{2}}\pi^{-\frac{1}{2}}\Gamma\left(\frac{1}{4}\right)^2.$$

这可通过下面的计算得知: 在此积分中作变量替换 $r = u^{\frac{1}{4}}$ 则有

$$\begin{aligned}\varpi &= \frac{1}{2}\int_0^1 u^{-\frac{3}{4}}(1-u)^{-\frac{1}{2}}du \\ &= \frac{1}{2}B\left(\frac{1}{4},\frac{1}{2}\right),\end{aligned}$$

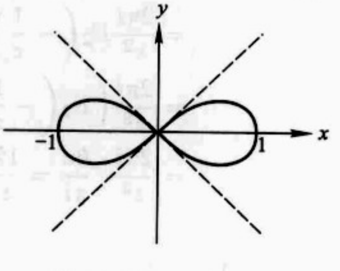


图 9.7

其中, 对于 $a, b > 0$,

$$B(a,b) = \int_0^1 u^{a-1}(1-u)^{b-1}du$$

为 β 函数, 我们有

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

其证明如下. 由

$$\Gamma(a) = \int_0^\infty x^{a-1}e^{-x}dx, \qquad \Gamma(b) = \int_0^\infty y^{b-1}e^{-y}dy$$

得到

$$\Gamma(a)\Gamma(b) = \int_0^\infty\int_0^\infty x^{a-1}y^{b-1}e^{-(x+y)}dxdy.$$

对其作变量替换

$$\begin{cases} x = ut & u\in[0,1],\ t\in[0,+\infty) \\ y = (1-u)t \end{cases}$$

则

$$\begin{aligned}\Gamma(a)\Gamma(b) &= \int_0^1 du\int_0^\infty tdt\cdot u^{a-1}(1-u)^{b-1}t^{a+b-2}e^{-t} \\ &= B(a,b)\Gamma(a+b).\end{aligned}$$

因此有

$$\varpi = \frac{1}{2}\frac{\Gamma\left(\frac{1}{4}\right)\Gamma\left(\frac{1}{2}\right)}{\Gamma\left(\frac{3}{4}\right)} = \frac{1}{2}\pi^{\frac{1}{2}}\Gamma\left(\frac{1}{4}\right)^2\frac{1}{\Gamma\left(\frac{1}{4}\right)\Gamma\left(\frac{3}{4}\right)},$$

再由公式

$$\Gamma(x)\Gamma(1-x)=\frac{\pi}{\sin \pi x}$$

便求出了

$$\varpi=\frac{1}{2}\pi^{\frac{1}{2}}\Gamma\left(\frac{1}{4}\right)^2\frac{\sin\frac{\pi}{4}}{\pi}=2^{-\frac{3}{2}}\pi^{-\frac{1}{2}}\Gamma\left(\frac{1}{4}\right)^2.$$

定理 9.16

(1) $\prod\limits_{m,n=-\infty}^{\infty}{}'\ (m^2+n^2)=4\pi^2\Delta(i)^6=4\pi^2e^{-\frac{\pi}{3}}\prod\limits_{n=1}^{\infty}(1-e^{-2\pi n})^4.$

(2) $\prod\limits_{m,n=-\infty}^{\infty}{}'\ (m^2+n^2)=2\varpi^2=\dfrac{\Gamma\left(\frac{1}{4}\right)^4}{4\pi}.$

(3) $\Delta(i)=e^{-2\pi}\prod\limits_{n=1}^{\infty}(1-e^{-2\pi n})^{24}=\left(\dfrac{\varpi}{\sqrt{2\pi}}\right)^{12}=\dfrac{\Gamma\left(\frac{1}{4}\right)^{24}}{2^{24}\pi^{18}}.$

(4) $E_4(i)=3\left(\dfrac{\varpi}{\pi}\right)^4=\dfrac{3\Gamma\left(\frac{1}{4}\right)^8}{64\pi^6}.$

(5) $\sum\limits_{m,n=-\infty}^{\infty}{}'\ \dfrac{1}{(mi+n)^4}=\dfrac{\varpi^4}{15}=\dfrac{\Gamma\left(\frac{1}{4}\right)^8}{960\pi^2}.$

(6) $\sum\limits_{n=1}^{\infty}\dfrac{n^3}{e^{2\pi n}-1}=\dfrac{1}{80}\left(\dfrac{\varpi}{\pi}\right)^4-\dfrac{1}{240}=\dfrac{\Gamma\left(\frac{1}{4}\right)^8}{5120\pi^6}-\dfrac{1}{240}.$

[证明] (1) 由在 Kronecker 极限公式 (定理 9.14) 中令 $z=i$, 而后取其平方即得. 但在取平方时, 我们使用了对于正规积来说, 如果 $c>0$, 则成立

$$\prod_{n=1}^{\infty}(a_n^c)=\left(\prod_{n=1}^{\infty}a_n\right)^c$$

的这个事实 (由定义立即得知).

(2) 使用在第七章 §7.5 中所证明的 Dedekind ζ 的分解

$$\zeta_{\mathbb{Q}(\sqrt{-1})}(s)=\zeta(s)L(s),$$
$$L(s)=L(s,\chi_{-1})=\sum_{n:\text{奇数}}(-1)^{\frac{n-1}{2}}n^{-s}.$$

像在第七章所看到的那样, 由于

$$\zeta_{\mathbb{Q}(\sqrt{-1})}(s)=\frac{1}{4}\sum_{m,n=-\infty}^{\infty}{}'\ (m^2+n^2)^{-s}$$

故

$$\prod_{m,n=-\infty}^{\infty}{}'\ (m^2+n^2)=\exp\left(-4\zeta'_{\mathbb{Q}(\sqrt{-1})}(0)\right).$$

我们来计算

$$\zeta'_{\mathbb{Q}(\sqrt{-1})}(0) = \zeta'(0)L(0) + \zeta(0)L'(0).$$

在第三章 §3.3, 我们已知

$$\zeta(0) = -\frac{1}{2}, \quad L(0) = \frac{1}{2},$$

又由推论 9.13 有

$$\zeta'(0) = -\frac{1}{2}\log(2\pi).$$

因此, 剩下的只是 $L'(0)$ 的计算. 利用

$$\begin{aligned} L(s) &= \sum_{m=0}^{\infty}(4m+1)^{-s} - \sum_{m=0}^{\infty}(4m+3)^{-s} \\ &= 4^{-s}\sum_{m=0}^{\infty}\left(m+\frac{1}{4}\right)^{-s} - 4^{-s}\sum_{m=0}^{\infty}\left(m+\frac{3}{4}\right)^{-s} \\ &= 4^{-s}\zeta\left(s,\frac{1}{4}\right) - 4^{-s}\zeta\left(s,\frac{3}{4}\right), \end{aligned}$$

于是

$$L'(0) = \zeta'\left(0,\frac{1}{4}\right) - \zeta'\left(0,\frac{3}{4}\right) - \log 4\left(\zeta\left(0,\frac{1}{4}\right) - \zeta\left(0,\frac{3}{4}\right)\right),$$

应用 Lerch 公式 (定理 9.12) (还有, $L(0) = \zeta\left(0,\frac{1}{4}\right) - \zeta\left(0,\frac{3}{4}\right) = \frac{1}{2}$), 则有

$$L'(0) = \log\frac{\Gamma\left(\frac{1}{4}\right)}{\sqrt{2\pi}} - \log\frac{\Gamma\left(\frac{3}{4}\right)}{\sqrt{2\pi}} - (\log 4)\frac{1}{2} = \log\frac{\Gamma\left(\frac{1}{4}\right)}{\Gamma\left(\frac{3}{4}\right)} - \log 2,$$

由公式

$$\frac{1}{\Gamma(x)\Gamma(1-x)} = \frac{\sin\pi x}{\pi}$$

得知

$$L'(0) = \log\left(\Gamma\left(\frac{1}{4}\right)^2 \cdot \frac{\sin\frac{\pi}{4}}{\pi}\right) - \log 2 = \log\left(\Gamma\left(\frac{1}{4}\right)^2 2^{-\frac{3}{2}}\pi^{-1}\right).$$

因此, 求出了

$$\zeta'_{\mathbb{Q}(\sqrt{-1})}(0) = -\frac{1}{4}\log\left(\frac{\Gamma\left(\frac{1}{4}\right)^4}{4\pi}\right).$$

于是得到了 (2) 中按 Γ 表示的那一部分, 从而按 ϖ 的表示的部分也就知道了.

(3) 由 (1) 和 (2) 推出.(这个公式是由 Lerch 在 1897 年发现的, 并由 Chowla-Selberg 于 1950 年左右重新发现.)

(4) 由 $E_4(i)=12\Delta(i)^{\frac{1}{3}}$ (§9.2(c), 推论 9.6) 得知.

(5) 由

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(mi+n)^4}=2\zeta(4)E_4(i)=\frac{\pi^4}{45}E_4(i)$$

得到. ∎

补充 1 将这里的等式汇集在以

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(mi+n)^4}=\sum_{m,n=-\infty}^{\infty}{}' \frac{m^4+n^4-6m^2n^2}{(m^2+n^2)^4}$$

为中心的计算里, 便有了下面这样的式子:

$$\begin{aligned}\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(mi+n)^4} &\underset{**}{=} \frac{\pi^4}{45}\left(1+240\sum_{n=1}^{\infty}\frac{n^3}{e^{2\pi n}-1}\right)\\ &\underset{***}{=} \frac{4\pi^4}{15}e^{-\frac{2\pi}{3}}\prod_{n=1}^{\infty}(1-e^{-2\pi n})^8\\ &\underset{****}{=} \frac{\Gamma\left(\frac{1}{4}\right)^8}{960\pi^2}\\ &\underset{*}{=} \frac{1}{15}\varpi^4.\end{aligned}$$

其中, $*$ 的数目表示了困难的程度. 请读者回想一下.

补充 2 使用 $E_8=E_4^2$ 同样可以求出

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m+ni)^{4k}}\qquad (k=1,2,\cdots)$$

(参看习题 9.3), 而 Hurwitz(1899年) 则利用椭圆曲线 $y^2=4x^3-4x$ 发展出了其他的方法. 我们在此作个简单的介绍 (同一个结果由几个不同的途径推导出来, 这在数论中经常发生, 而这种等价性暗含着某种深刻的事实). 对于椭圆曲线请参看第十二章. 我们现在考虑的椭圆曲线是方程

$$y^2=4x^3-g_2x-g_3$$

中 $g_2=4,\ g_3=0$ 的情形. 这时 $\wp$ 函数

$$\wp(u)=\frac{1}{u^2}+\sum_{m,n=-\infty}^{\infty}{}' \left\{\frac{1}{(u-(m+ni)\varpi)^2}-\frac{1}{((m+ni)\varpi)^2}\right\}$$

满足微分方程

$$\wp'(u)^2 = 4\wp(u)^3 - 4\wp(u).$$

又, 在 $u=0$ 处展开其 Laurent 级数则有

$$\wp(u) = \frac{1}{u^2} + \sum_{k=1}^{\infty}(4k-1)\left(\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{((m+ni)\varpi)^{4k}}\right)u^{4k-2}.$$

因此令

$$\sum_{m,n=-\infty}^{\infty} \frac{1}{(m+ni)^{4k}} = \frac{(2\varpi)^{4k}}{(4k)!}e_k$$

(这是 $\mathbb{Q}\left(\sqrt{-1}\right)$ 的 L 函数的特殊值), 则因为

$$\wp(u) = \frac{1}{u^2} + \sum_{k=1}^{\infty}\frac{2^{4k}e_k}{4k}\cdot\frac{u^{4k-2}}{(4k-2)!} = \frac{1}{u^2} + 2e_1u^2 + \frac{2e_2}{45}u^6 + \cdots,$$

$$\wp''(u) = \frac{6}{u^4} + \sum_{k=1}^{\infty}\frac{2^{4k}e_k}{4k}\cdot\frac{u^{4k-4}}{(4k-4)!} = \frac{6}{u^4} + 4e_1 + \frac{4}{3}e_2u^4 + \cdots,$$

利用微分方程

$$\wp''(u) = 6\wp(u)^2 - 2$$

得到递推公式解

$$e_1 = \frac{1}{10},$$

$$(2k-3)(4k-1)(4k+1)e_k = 3\sum_{l=1}^{k-1}(4l-1)(4k-4l-1)\binom{4k}{4l}e_le_{k-l}.$$

由此, 譬如可以知道

$$4e_1 = 24e_1 - 2, \quad \frac{4}{3}e_2 = 24e_1^2 + \frac{8}{15}e_2, \cdots.$$

于是求出了

$$e_1 = \frac{1}{10},\ e_2 = \frac{3}{10},\ e_3 = \frac{567}{130},$$
$$e_4 = \frac{43659}{170},\ e_5 = \frac{392931}{10}, \ldots$$

那么,

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m+ni)^4} = \frac{\varpi^4}{15}$$

等等便可求出. 称 e_k 为 Hurwitz 数, 我们已知其与 Bernoulli 数 B_k 同样具有深刻的数论意义 (Coates–Wiles, 1977年).

补充 3 ϖ 是 Gauss(1799年) 由研究算术几何平均数时发现的量, 作为自守形式/椭圆函数论发端的事件是应该被纪念的. 我们从历史的意义上介绍一下 ϖ 与算术几何平均的关系.

当给出正数 $a \geqslant b$ 时, 由 $a_0 = a,\ b_0 = b$ 递推地定义数列 $\{a_n\}, \{b_n\}$ 如下:

$$\begin{cases} a_{n+1} = \dfrac{a_n + b_n}{2} & (\text{算术平均}) \\ b_{n+1} = \sqrt{a_n b_n} & (\text{几何平均}), \end{cases}$$

成立 $a_0 \geqslant a_1 \geqslant a_2 \geqslant \cdots \geqslant b_2 \geqslant b_1 \geqslant b_0$ 及

$$|a_n - b_n| \leqslant \frac{a_0 - b_0}{2^n},$$

于是得知 $\lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} b_n$. 称此极限值为**算术几何平均** (arithmetico-geometric mean), 以 $\mathrm{AGM}(a,b)$ 记之.

Gauss 发现的是

$$\mathrm{AGM}(\sqrt{2}, 1) = \frac{\pi}{\varpi}$$

这个等式. 更一般地 Gauss 得到了 $\mathrm{AGM}(a,b)$ 的公式.

定理 9.17 (Gauss)

$$\mathrm{AGM}(a,b) = \frac{\dfrac{\pi}{2}}{\displaystyle\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{a^2\cos^2\theta + b^2\sin^2\theta}}}.$$

[证明] 将上式右端的倒数记为 $F(a,b)$. 以 $x = b\tan\theta$ 作替换, 有

$$F(a,b) = \frac{2}{\pi}\int_0^{\infty} \frac{dx}{\sqrt{(a^2+x^2)(b^2+x^2)}} = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{dx}{\sqrt{(a^2+x^2)(b^2+x^2)}}.$$

进一步作替换 $y = \dfrac{1}{2}\left(x - \dfrac{ab}{x}\right)$ 则有

$$F(a,b) = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{dy}{\sqrt{\left(\left(\dfrac{a+b}{2}\right)^2 + y^2\right)(ab+y^2)}} = F\left(\frac{a+b}{2}, \sqrt{ab}\right).$$

因此有

$$F(a,b) = F(a_1,b_1) = F(a_2,b_2) = \cdots = F(a_n,b_n).$$

于是, 令 $\mathrm{AGM}(a,b) = \alpha$ 则

$$F(a,b) = \lim_{n\to\infty} F(a_n,b_n) = F(\alpha,\alpha) = \frac{2}{\pi}\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{\alpha^2\cos^2\theta + \alpha^2\sin^2\theta}} = \frac{1}{\alpha},$$

则知 $\mathrm{AGM}(a,b) = F(a,b)^{-1}$.

特别地, 有

$$\begin{aligned}\mathrm{AGM}(\sqrt{2},1)^{-1} &= \frac{2}{\pi}\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1+\cos^2\theta}} = \frac{2}{\pi}\int_0^1 \frac{du}{\sqrt{1-u^4}} \quad (u=\cos\theta)\\ &= \frac{\varpi}{\pi}.\end{aligned}$$

另外, 公式 $F(a,b)=F\left(\dfrac{a+b}{2},\sqrt{ab}\right)$ 是椭圆函数的 “加法公式” 之一.

§9.6 $SL_2(\mathbb{Z})$ 的自守形式

我们来罗列模群(modular group) $\Gamma = SL_2(\mathbb{Z})$ 的基本性质与相关的自守形式. 自守形式作为全纯的与实解析的对象, 这两点中的任一点在数论中都是非常重要的.

(a) $SL_2(\mathbb{Z})$ 的基本性质

定理 9.18

$$SL_2(\mathbb{Z}) = \left\langle \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}0&-1\\1&0\end{pmatrix} \right\rangle.$$

[证明] 设 $\gamma = \begin{pmatrix}a&b\\c&d\end{pmatrix} \in SL_2(\mathbb{Z})$.

(1) 当 $c=0$ 时, 则有 $a=d=\pm1$, 于是

$$\begin{aligned}\gamma = \begin{pmatrix}1&b\\0&1\end{pmatrix} &= \begin{pmatrix}1&1\\0&1\end{pmatrix}^b,\\ \gamma = \begin{pmatrix}-1&b\\0&-1\end{pmatrix} &= \begin{pmatrix}1&-b\\0&1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}^2\\ &= \begin{pmatrix}1&1\\0&1\end{pmatrix}^{-b}\begin{pmatrix}0&-1\\1&0\end{pmatrix}^2,\end{aligned}$$

这时定理成立.

(2) 当 $c \geqslant 1$ 时, 对于 c 使用归纳法. 如果 $c=1$, 则

$$\begin{aligned}\gamma = \begin{pmatrix}a&ad-1\\1&d\end{pmatrix} &= \begin{pmatrix}1&a\\0&1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&d\\0&1\end{pmatrix}\\ &= \begin{pmatrix}1&1\\0&1\end{pmatrix}^a\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}^d.\end{aligned}$$

如果 $c \geqslant 2$, 由于 $(c,d)=1$, 故可表 d 为 $d=cq+r$, $1 \leqslant r \leqslant c-1$, 于是

$$\begin{aligned}\gamma = & \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-q}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q} \\ = & \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q} \\ = & \begin{pmatrix} -aq+b & -q \\ r & -c \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q}.\end{aligned}$$

由归纳假定知, $\gamma \in \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$.

(3) $c \leqslant -1$ 的情形: 此时有

$$\gamma = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{2},$$

因为 $-c \geqslant 1$ 故可应用 (2). ∎

定理 9.19 令

$$\begin{aligned} D = & \left\{ x+iy \,\middle|\, -\frac{1}{2} < x < \frac{1}{2},\ y > \sqrt{1-x^2} \right\} \\ & \sqcup \left\{ -\frac{1}{2} + iy | y > \frac{\sqrt{3}}{2} \right\} \sqcup \left\{ x + i\sqrt{1-x^2} | -\frac{1}{2} \leqslant x \leqslant 0 \right\}, \end{aligned}$$

则

$$SL_2(\mathbb{Z}) \backslash H = D.$$

[证明] 对于 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ 与 $z \in H$ 令 $\gamma z = \dfrac{az+c}{cz+d}$. 只要证明以下的 (1),(2) 即可.

(1) 对于 $z \in H$ 存在 $\gamma \in \Gamma$ 使得 $\gamma z \in D$.

(2) 如果 $z, \gamma z \in D$, 则 $z = \gamma z$. (就是说, 对于 $z_1, z_2 \in D$, 如果 $\gamma z_1 = z_2$ 则 $z_1 = z_2$.)

(1) 的证明: 固定 $z \in H$. 对于 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 有

$$\operatorname{Im}(\gamma z) = \frac{\operatorname{Im}(z)}{|cz+d|^2}$$

且因为

$$|cz+d|^2 = (cx+d)^2 + (cy)^2,$$

故可取某个 $\gamma_1 \in \Gamma$ 使得 $\mathrm{Im}(\gamma_1 z)$ 达到最大. 另外还可以选取 $n \in \mathbb{Z}$ 使得 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \gamma_1 z$ 的实部落在 $\left[-\frac{1}{2}, \frac{1}{2}\right)$ 之中. 那么,

$$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \gamma_1$$

便为所求. 要证明此断言, 只要证明 $|\gamma z| \geqslant 1$ 就可以了. 而如果 $|\gamma z| < 1$, 则会有

$$\mathrm{Im}\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \gamma z\right) = \mathrm{Im}\left(-\frac{1}{\gamma z}\right) = \frac{\mathrm{Im}(\gamma z)}{|\gamma z|^2} > \mathrm{Im}(\gamma z) = \mathrm{Im}(\gamma_1 z),$$

与所取 γ_1 的条件相矛盾.

(2) 的证明: 只要证明 $\mathrm{Im}(\gamma z) \geqslant \mathrm{Im}(z)$ 的情形即可 (如果不是这样, 则转而考虑 $\gamma^{-1}z$ 与 z 这一对). 于是, 设 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 则有 $|cz+d| \leqslant 1$. 那么, 因为 $x^2+y^2 \geqslant 1$, $-\frac{1}{2} \leqslant x < \frac{1}{2}$, 故由

$$\begin{aligned}|cz+d|^2 &= c^2(x^2+y^2) + 2cdx + d^2 \\ &\geqslant c^2 - |cd| + d^2 = \left(|d| - \frac{|c|}{2}\right)^2 + \frac{3c^2}{4} \geqslant \frac{3c^2}{4}\end{aligned}$$

知有 $c = 0, \pm 1$.

(i) $c=0$ 的情形: 此时, $\gamma = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$ 从而 $\gamma z = z + n$, 如果观察其实部, 则必定有 $n=0$. 因此, $\gamma = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 故 $\gamma z = z$.

(ii) $c=1$ 的情形: 此时, $|z+d| \leqslant 1$, 观察图 9.1 知道, 这样的 d 和 z 仅仅有

$$\begin{cases} \text{在 } d=0, \text{ 有 } |z|=1, \text{ (因此, } -\frac{1}{2} \leqslant x \leqslant 0) \\ \text{如果 } d \neq 0 \text{ 则 } d=1, \text{ 从而 } z = \rho = \dfrac{-1+\sqrt{3}i}{2}. \end{cases}$$

上面的情形即为 $\gamma = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$, 而

$$\gamma z = \frac{az-1}{z} = a - \frac{1}{z} = a - \bar{z}$$

只在 $z=i$, $a=0$ 或者 $z=\rho$, $a=-1$ 时才属于 D. 此时, 只在 $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $z=i$ 或者在 $\gamma = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $z=\rho$ 时, 能使得 $\gamma z = z$. 下面的情形由 $\gamma = \begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix}$ 有

$a-b=1$, 由于

$$\begin{aligned}\gamma\rho=\frac{a\rho+b}{\rho+1}&=-\rho(a\rho+b)=-a\rho^2-b\rho\\&=a(\rho+1)-b\rho=(a-b)\rho+a\\&=\rho+a\end{aligned}$$

从而仅当 $a=0$ 时才属于 D. 于是, 此时在 $\gamma=\begin{pmatrix}0&-1\\1&1\end{pmatrix}$, $z=\rho$ 时有 $\gamma z=z$.

(iii) $c=-1$ 的情形: 此时考虑 $-\gamma$, 从而化到 (ii) 即可. ∎

(b) 全纯自守形式

为简单起见, 对于 $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ 和 $z\in H$, 令 $j(\gamma,z)=cz+d$.

对于整数 $k\geqslant 0$, 构造两个 $\mathbb{C}$ 线性空间:

$$M_k(\Gamma)=\left\{f:H\to\mathbb{C}\text{全纯}\;\middle|\;\begin{matrix}(1)\text{ 对于所有 }\gamma\in\Gamma\text{ 有 }f(\gamma z)=j(\gamma,z)^kf(z)\\(2)\text{ 具有 Fourier 展开 }f(z)=\sum_{n=0}^{\infty}a(n,f)q^n.\end{matrix}\right\}$$

$$\bigcup$$

$$S_k(\Gamma)=\left\{f:H\to\mathbb{C}\text{全纯}\;\middle|\;\begin{matrix}(1)\text{ 对于所有 }\gamma\in\Gamma\text{ 有 }f(\gamma z)=j(\gamma,z)^kf(z)\\(2)\text{ 具有 Fourier 展开 }f(z)=\sum_{n=1}^{\infty}a(n,f)q^n.\end{matrix}\right\}$$

称 $M_k(\Gamma)$ 中的元为权 k 的**全纯模形式** (holomorphic modular form)(本书中也不加区别地称其为**全纯自守形式** — 译注), 而称 $S_k(\Gamma)$ 中的元为**全纯尖点形式** (holomorphic cusp form). 所谓 "尖点形式" 指的是尖点 $i\infty$ "$f(i\infty)=a(0,f)=0$" 消失. 当 k 为奇数时, 在 $\gamma=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ 作用下有 $f(z)=(-1)^kf(z)=-f(z)$, 故而 $f=0$. 以下设 $k\geqslant 0$ 为偶数.

自守形式的变换公式的条件只要对 Γ 的生成元 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ 满足就够了, 也就是说只要知道成立

$$\begin{cases}f(z+1)=f(z)\\f\left(-\dfrac{1}{z}\right)=z^kf(z)\end{cases}$$

即可. 由于其中的 $f(z+1)=f(z)$ 被包含在 Fourier 展开的条件之中, 便有如下结果:

$$M_k(\Gamma)=\left\{ f:H\to\mathbb{C} \;\middle|\; \begin{array}{l}(1)\, f\left(-\dfrac{1}{z}\right)=z^k f(z)\\ (2)\, f(z)=\displaystyle\sum_{n=0}^{\infty}a(n,f)q^n.\end{array}\right\}$$

$$\bigcup$$

$$S_k(\Gamma)=\left\{ f:H\to\mathbb{C} \;\middle|\; \begin{array}{l}(1)\, f\left(-\dfrac{1}{z}\right)=z^k f(z)\\ (2)\, f(z)=\displaystyle\sum_{n=1}^{\infty}a(n,f)q^n.\end{array}\right\}$$

再者, 对于只需看生成元即可这样的说法还需弄清. 当给出了一般的 $\gamma_1,\gamma_2\in\Gamma$ 时, 如果

$$\begin{cases} f(\gamma_1 z)=f(z)j(\gamma_1,z)^k\\ f(\gamma_2 z)=f(z)j(\gamma_2,z)^k,\end{cases}$$

则要能够成立

$$f((\gamma_1\gamma_2)z)=f(z)j(\gamma_1\gamma_2,z)^k$$

才行; 对其进行具体的计算, 则确定应该成立

$$\begin{cases} (\gamma_1\gamma_2)z=\gamma_1(\gamma_2 z)\\ j(\gamma_1\gamma_2,z)=j(\gamma_1,\gamma_2 z)j(\gamma_2,z).\end{cases}$$

定理 9.20 设 $k\geqslant 0$ 为偶数.

(1)
$$M_k(\Gamma)=\bigoplus_{\substack{4a+6b=k\\ a,b\geqslant 0}}\mathbb{C}E_4^aE_6^b.$$

(2) 对于 $k\geqslant 4$, 有

$$M_k(\Gamma)=\mathbb{C}\cdot E_k\oplus S_k(\Gamma),$$

而如果 $k\geqslant 12$ 则

$$M_k(\Gamma)=\mathbb{C}\cdot E_k\oplus\Delta\cdot M_{k-12}(\Gamma).$$

(3)

$$\dim_{\mathbb{C}}M_k(\Gamma)=\begin{cases}\left[\dfrac{k}{12}\right]+1 & k\not\equiv 2 \mod 12\\ \left[\dfrac{k}{12}\right] & k\equiv 2 \mod 12.\end{cases}$$

[证明] 为简单起见, 略去 $\Gamma = SL_2(\mathbb{Z})$ 记为 M_k 以及 S_k. 按下面 (i)–(vi) 的顺序证明:

(i) $k < 12$ 时, $S_k = 0$,

(ii) $k \geqslant 12$ 时, $S_k = \Delta \cdot M_{k-12}$,

(iii) (2) 成立,

(iv) $k < 12$ 时 (1) 成立,

(v) (3) 成立,

(vi) (1) 成立.

(i) 对于 $f \in S_k$, 考虑 $F = \dfrac{f^{12}}{\Delta^k}$. 那么它在 $\Gamma\backslash H \cup \{i\infty\}$ 全纯, 且因为 $k < 12$ 故在 $i\infty$ 其为 0. 因此, $F = 0$ 从而 $f = 0$.

(ii) 对于 $f \in S_k$, 考虑 $h = \dfrac{f}{\Delta}$, 于是 $h \in M_{k-12}$.

(iv) 当 $k \geqslant 4$ 时, 取 $f \in M_k$ 则 $h = f - a(0,f)E_k \in S_k$. 因此可记为 $f = a(0,f)E_k + h$, $h \in S_k$, 至于直和, 看一看常数项就知道了. (2) 的后半部分用 (ii) 即可完成.

(iv) 我们断言 $M_0 = \mathbb{C}$, $M_2 = 0$, $M_4 = \mathbb{C}E_4$, $M_6 = \mathbb{C}E_6$, $M_8 = \mathbb{C}E_8 = \mathbb{C}E_4^2$, $M_{10} = \mathbb{C}E_{10} = \mathbb{C}E_4E_6$. 首先, 当 $k = 4,6,8,10$ 时取 $f \in M_k$, 由于 $f - a(0,f)E_k \in S_k = 0$ 故 $f = a(0,f)E_k$. 进而 $E_8 = E_4^2$, $E_{10} = E_4E_6$ 各自由 $E_8 - E_4^2 \in S_8 = 0$, $E_{10} - E_4E_6 \in S_{10} = 0$ 得知. M_0 的元在 $\Gamma\backslash H\bigcup\{i\infty\}$ 为全纯函数, 因而仅为常数. 现来证 $M_2 = 0$. 取 $f \in M_2$. 此时 $fE_4 \in M_6 = \mathbb{C}E_6$ 故 $fE_4 = cE_6$. 在其中令 $z = \rho = \dfrac{-1+\sqrt{3}i}{2}$, 则有 $f(\rho)E_4(\rho) = c \cdot E_6(\rho)$, 则因为 $E_4(\rho) = 0$, $E_6(\rho) \neq 0$ 知 $c = 0$. 从而 $f = 0$. ($E_k(\rho)$ 的计算与 $E_k(i)$ 的计算相同. 参看习题 9.4.)

(v) 当 $k < 12$ 时, (3) 由 (iv) 可得. 而后由 (ii) ((2) 的后半部), 因为当 $k \geqslant 12$ 时

$$\dim M_k = \dim M_{k-12} + 1,$$

故得到 (3) 的一般情形.

(vi) 至于 $\mathbb{C}E_4^aE_6^b$ 的和为直和, 我们假设有 $c(a_i,b_i) \neq 0$, $(i = 1,\cdots,r)$ 使得

$$c(a_1,b_1)E_4^{a_1}E_6^{b_1} + \cdots + c(a_r,b_r)E_4^{a_r}E_6^{b_r} = 0,\ a_1 > a_2 > \cdots > a_r,$$

那么对其除以 $E_6^{b_1}$ 则有

$$c(a_1,b_1)E_4^{a_1} + c(a_2,b_2)E_4^{a_2}E_6^{b_2-b_1} + \cdots + c(a_r,b_r)E_4^{a_r}E_6^{b_r-b_1} = 0,$$

若在其中代入 $z = i$, 则有 $c(a_1,b_1) = 0$, 从而产生矛盾而得知. 又,

$$M_k \subset \bigoplus_{\substack{4a+6b=k \\ a,b\geqslant 0}} \mathbb{C}E_4^aE_6^b$$

可由 (2) 的构造和 $\Delta=\dfrac{E_4^3-E_6^2}{1728}$ 得到. ∎

注记 回顾一下这个证明, 它也导出了

$$\#\{(a,b)\mid a,b\geqslant 0, 4a+6b=k\}=\begin{cases}\left[\dfrac{k}{12}\right]+1 & k\not\equiv 2 \mod 12\\ \left[\dfrac{k}{12}\right] & k\equiv 2 \mod 12.\end{cases}$$

关于 Δ 或 E_k 所叙述的事实也可以推广到对于权 k 自守形式. 证明几乎不用改变. 我们来把要点概要地看一下. 首先对于 $m\geqslant 1$, 将 Mordell 算子 $T(p)$ 推广为 **Hecke 算子** (Hecke operator)

$$T_k(m): M_k(\Gamma)\to M_k(\Gamma),$$

其定义为

$$\begin{aligned}(T_k(m)f)(z)&=m^{k-1}\sum_{ad=m}\sum_{b=0}^{d-1}d^{-k}f\left(\frac{az+b}{d}\right)\\&=\sum_{n=0}^{\infty}\left(\sum_{d|(m,n)}d^{k-1}a\left(\frac{mn}{d^2},f\right)\right)q^n\\&=\sigma_{k-1}(m)a(0,f)+\sum_{n=1}^{\infty}\left(\sum_{d|(m,n)}d^{k-1}a\left(\frac{mn}{d^2},f\right)\right)q^n.\end{aligned}$$

称

$$\mathbb{T}_k=\mathbb{C}[T_k(m)\mid m=1,2,\cdots]\subset \mathrm{End}_{\mathbb{C}}(M_k(\Gamma))$$

为 **Hecke 环**. 由关系式

$$T_k(m)T_k(n)=T_k(n)T_k(m)=\sum_{d|(m,n)}d^{k-1}T_k\left(\frac{mn}{d^2}\right)$$

知 $\mathbb{T}_k$ 为交换 $\mathbb{C}$ 代数. (另外, Hecke 环在 $S_k(\Gamma)$ 的限制以及局部的类比等等都有着各种各样的意义.) 当 $f\in M_k(\Gamma)$ 同时为所有 $T_k(m)$ $(m=1,2,\cdots)$ 的特征函数

$$T_k(m)f=\lambda(m,f)f$$

时, 称

$$L(s,f)=\sum_{m=1}^{\infty}\lambda(m,f)m^{-s}=\prod_p(1-\lambda(p,f)p^{-s}+p^{k-1-2s})^{-1}$$

为 f 的 L 函数. $f=E_k$ 时有 $T_k(m)E_k=\sigma_{k-1}(m)E_k$, 故 $L(s,E_k)=\zeta(s)\zeta(s-k+1)$. 当 f 为非零尖点形式时, 利用 $a(m,f)=\lambda(m,f)a(1,f)$, 则成立积分表示

$$\begin{aligned}\widehat{L}(s,f)&=(2\pi)^{-s}\Gamma(s)L(s,f)\\&=a(1,f)^{-1}\int_1^{\infty}f(iy)(y^s+(-1)^{\frac{k}{2}}y^{k-s})\frac{dy}{y},\end{aligned}$$

因而得到了其在全平面全纯以及 $s \leftrightarrow k-s$ 式的函数方程

$$\widehat{L}(s,f) = (-1)^{\frac{k}{2}}\widehat{L}(k-s,f).$$

另外, 尖点形式的空间 $S_k(\Gamma)$ 具有 **Petersson 内积** (Petersson inner product)

$$\langle f,g\rangle = \mathrm{vol}(\Gamma\backslash H)^{-1}\int_{\Gamma\backslash H} f(z)\overline{g(z)}y^k\frac{dxdy}{y^2}$$

(注意使用在 §9.4(c) 的 Rankin–Selberg 方法). 这里的

$$\begin{aligned}\mathrm{vol}(\Gamma\backslash H) &= \int_{\Gamma\backslash H}\frac{dxdy}{y^2}\\ &= \int_{-\frac{1}{2}}^{\frac{1}{2}}\left(\int_{\sqrt{1-x^2}}^{\infty}\frac{dy}{y^2}\right)dx = \int_{-\frac{1}{2}}^{\frac{1}{2}}\frac{dx}{\sqrt{1-x^2}} = \frac{\pi}{3}.\end{aligned}$$

相对于此内积而言, $T_k(m)$ 成为了 Hermite 算子, 即有 $\langle T_k(m)f,g\rangle = \langle f,T_k(m)g\rangle$. 于是, $T_k(m)$ $(m=1,2,\cdots)$ 是互换的 Hermite 算子, 具有由共同特征函数构成的基底. 还有, $T_k(m)$ 的特征值为实数, 由 $S_k(\Gamma)(M_k(\Gamma))$ 可取整数基底 $E_4^aE_6^b\Delta^c$ (但, 若 $k\equiv 0 \mod 4$ 则 $b=0$, $k\equiv 2 \mod 4$ 时则 $b=1$), 那么它的特征值为全实代数整数.

另外, Hecke 逆定理 (§9.3(b) 的定理 9.8) 有下面的推广.

定理 9.21 (Hecke) 设 $k>0$ 为偶数. 对于复数序列 $\boldsymbol{a}=(a(1),a(2),a(3),\cdots)$, 令

$$\begin{aligned}f_{\boldsymbol{a}}(z) &= \sum_{n=1}^{\infty}a(n)q^n,\\ L(s,\boldsymbol{a}) &= \sum_{n=1}^{\infty}a(n)n^{-s},\\ \widehat{L}(s,\boldsymbol{a}) &= (2\pi)^{-s}\Gamma(s)L(s,\boldsymbol{a}).\end{aligned}$$

于是, 下面的 (A) 与 (B) 等价:

(A) $f_{\boldsymbol{a}}\in S_k(\Gamma)$.

(B) (1) 对于某个 $\gamma>0$, 有 $a(n)=O(n^{\gamma})$.

(2) $\widehat{L}(s,\boldsymbol{a})$ 在整个 s 平面全纯, 且 $\widehat{L}(k-s,\boldsymbol{a}) = (-1)^{\frac{k}{2}}\widehat{L}(s,\boldsymbol{a})$.

(3) $\widehat{L}(s,\boldsymbol{a})$ 在任意竖直区域有界.

[证明] 在定理 9.8 的证明中有 12 的地方换成用 k 去做就可以了. (再者, 对于 $f\in S_k(\Gamma)$, 可以给出估值 $a(n,f)=O(n^{\frac{k}{2}})$.) ∎

(c) 实解析的自守形式

在 $\Gamma = SL_2(\mathbb{Z})$ 的自守形式中有所谓的实解析的 Maass **波动形式** (wave form).

这是 Maass(1949年) 所构建的理论. 所谓波动形式的空间是对于复数 r 所定义的

$$W_r(\Gamma)=\left\{f:H\to\mathbb{C}\text{为实解析}\;\middle|\;\begin{array}{l}(1)\ f(\gamma z)=f(z)\text{对所有的 }\gamma\in\Gamma\text{ 成立}\\(2)\ \Delta_\Gamma f=\left(\dfrac{1}{4}+r^2\right)f\\(3)\ f(z)=O(y^c)\text{对于 }y\to+\infty\text{ 成立 }(c\text{ 为常数}).\end{array}\right\}$$

其中

$$\Delta_\Gamma=-y^2\left(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}\right)$$

为 Laplace 算子. (当其为全纯自守形式时, 考虑所谓的 Cauchy-Riemann 方程的微分方程, 便容易了解到这一点.)

此时, 根据 (1) 的 $f(z+1)=f(z)$ 及 (3) 的条件, 则有 Fourier 展开

$$f(z)=\sum_{m=-\infty}^{\infty}a(m,y)e^{2\pi imx},$$

解 (2) 的微分方程, 求出 $a(m,y)$ 来, 则有

$$W_r(\Gamma)=\left\{f:H\to\mathbb{C}\;\middle|\;\begin{array}{l}(1)\ f\left(-\dfrac{1}{z}\right)=f(z)\\(2)\ f(z)=ay^{\frac{1}{2}+ir}+by^{\frac{1}{2}-ir}\\\qquad+\displaystyle\sum_{m=-\infty}^{\infty}{}'\,a(m)\sqrt{y}K_{ir}(2\pi|m|y)e^{2\pi imx}.\end{array}\right\}$$

其中, 当 $r=0$ 时上面 (2) 为

$$f(z)=ay^{\frac{1}{2}}+by^{\frac{1}{2}}\log y+\sum_{m=-\infty}^{\infty}{}'\,a(m)\sqrt{y}K_0(2\pi|m|y)e^{2\pi imx}.$$

(实际上, $SL_2(\mathbb{Z})$ 的情形不会发生 $r=0$, 而是出现在同余子群时的重要情形.) $W_r(\Gamma)$ 之中的尖点形式所形成的子空间为

$$W_r^0(\Gamma)=\left\{f:H\to\mathbb{C}\;\middle|\;\begin{array}{l}(1)\ f\left(-\dfrac{1}{z}\right)=f(z)\\(2)\ f(z)=\displaystyle\sum_{m=-\infty}^{\infty}{}'\,a(m)\sqrt{y}K_{ir}(2\pi|m|y)e^{2\pi mx}.\end{array}\right\}$$

譬如, $E\left(\frac{1}{2}+ir,z\right)$ 为 $W_r(\Gamma)$ 的元. 并且, 使得 $W_r^0(\Gamma)\neq 0$ 的 $r\in\mathbb{C}$ — 它恰好使得 $\frac{1}{4}+r^2$ 为 Laplace 算子的特征值— 全为纯虚数且知为可数无限多个. 进一步我们还知, Hecke 算子 $T(n):W_r(\Gamma)\to W_r(\Gamma)$ 由

$$(T(n)f)(z)=\frac{1}{\sqrt{n}}\sum_{ad=n}\sum_{b=0}^{d-1}f\left(\frac{az+b}{d}\right)$$

确定, 它成为关于 **Petersson 内积**

$$\langle f,g\rangle=\int_{\Gamma\backslash H}f(z)\overline{g(z)}\frac{dxdy}{y^2}$$

的 Hermite 算子. 对于它们的共同特征函数 f, 其 L 函数 $L(s,f)$ 具有好的解析性质, 且逆定理成立. 例如, 我们有 $L(s,E(\frac{1}{2}+ir,\cdot))=\zeta(s+ir)\zeta(s-ir)$. 所有这些都是 Maass 的结果. 再者, 我们也推测成立类似的 Ramanujan 猜想, 但这里不可能使用代数几何的手段, 它至今仍未得到证明.

§9.7 经典的自守形式

(a) 同余子群的情形

称 $SL_2(\mathbb{Z})$ 的子群

$$\Gamma(N)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})\,\middle|\,\begin{pmatrix}a&b\\c&d\end{pmatrix}\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}\mod N\right\}$$

为 N 级的主同余子群 (考虑对每个分量的同余). $\Gamma(1)=SL_2(\mathbb{Z})$, 而 $\Gamma(N)$ 为 $SL_2(\mathbb{Z})$ 的具有有限指数的正规子群.

一般地, 称满足

$$SL_2(\mathbb{Z})\supset\Gamma\supset\Gamma(N)$$

的群 Γ 为**同余子群** (congruence subgroup). 它们也是有限生成的群. 在 $SL_2(\mathbb{Z}),\Gamma(N)$ 之外还常使用

$$\Gamma_0(N)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})\,\middle|\,\begin{pmatrix}a&b\\c&d\end{pmatrix}\equiv\begin{pmatrix}*&*\\0&*\end{pmatrix}\mod N\right\}\supset\Gamma(N).$$

对于这样一些同余子群也有对应于 §9.6 的自守形式的理论 (全纯的, 实解析的), 也可以考虑对应的 Hecke 算子以及 L 函数. 然而, Fourier 展开则处理了在被称做尖点的 $\Gamma\backslash(\mathbb{Q}\cup\{i\infty\})$ 的所有点 (有限个) 处的展开而不仅限于在 $i\infty$. 再者, 我们实际上有 $SL_2(\mathbb{Z})\backslash(\mathbb{Q}\cup\{i\infty\})=\{i\infty\}$, 故而在 $SL_2(\mathbb{Z})$ 时, 尖点只有 $i\infty$. 至于 Hecke 算子以及 L 函数的因式对于使 $p|N$ 的素数 p (称为 "坏的素数") 形式有所变化 (Euler 积可以退化为不大于一次的因式), 而其他地方与 $SL_2(\mathbb{Z})$ 几乎都一样.

由于篇幅的关系, 在这里我们不去介绍它们的理论, 而替代地, 看一下作为同余子群的自守形式典型例子的 ϑ 级数及其作为应用而出现的 Jacobi 四平方定理.

一般地, 对于自然数 k 令

$$r_k(n)=\#\{(n_1,\cdots,n_k)\in\mathbb{Z}^k\mid n_1^2+\cdots+n_k^2=n\}.$$

这是将 n 表示成 k 个平方和的方法的总个数 (算上符号), 利用 ϑ 级数

$$\vartheta(z)=\sum_{n=-\infty}^{\infty}e^{\pi i n^2 z}=\sum_{n=-\infty}^{\infty}q^{\frac{n^2}{2}}\quad(q=e^{2\pi iz}),$$

则因为

$$\begin{aligned}\vartheta(z)^k&=\left(\sum_{n=-\infty}^{\infty}q^{\frac{n^2}{2}}\right)^k\\&=\left(\sum_{n_1=-\infty}^{\infty}q^{\frac{n_1^2}{2}}\right)\cdots\cdots\left(\sum_{n_k=-\infty}^{\infty}q^{\frac{n_k^2}{2}}\right)\\&=\sum_{n_1,\cdots,n_k=-\infty}^{\infty}q^{\frac{n_1^2+\cdots+n_k^2}{2}}\\&=\sum_{n=0}^{\infty}r_k(n)q^{\frac{n^2}{2}},\end{aligned}$$

于是, 求 $r_k(n)$ 的问题变成了求权 $\frac{k}{2}$ 的自守形式 $\vartheta(z)^k$(2 级) 的表示问题了.

$k=2$ 的情形, 由§7.6 的 Dedekind ζ 的计算

$$\zeta_{\mathbb{Q}(\sqrt{-1})}(s)=\zeta(s)L(s,\chi_{-1})$$

知道有

$$r_2(n)=4\sum_{\substack{d|n\\d:\text{奇数}}}\chi_{-1}(d)=4\sum_{\substack{d|n\\d:\text{奇数}}}(-1)^{\frac{d-1}{2}}.$$

注意, 这个关系式可写为

$$(*)\qquad \vartheta(z)^2=\left(\sum_{n=-\infty}^{\infty}q^{\frac{n^2}{2}}\right)^2=1+4\sum_{m=1}^{\infty}(-1)^{m-1}\frac{q^{(2m-1)/2}}{1-q^{(2m-1)/2}}.$$

这是个 "ϑ 级数 =Eisenstein 级数" 的等式. (Eisenstein 级数如在 §9.1(c) 所见的那样, 容易知道其可写成 Lambert 级数.) 实际上, 我们有

$$\begin{aligned}\left(\sum_{n=-\infty}^{\infty}q^{n^2/2}\right)^2&=1+\sum_{n=1}^{\infty}r_2(n)q^{n/2}\\&=1+4\sum_{n=1}^{\infty}\left(\sum_{\substack{d|n\\d:\text{奇数}}}(-1)^{\frac{d-1}{2}}\right)q^{n/2}\\&=1+4\sum_{m=1}^{\infty}(-1)^{m-1}\sum_{n=1}^{\infty}q^{(2m-1)n/2}\\&=1+4\sum_{m=1}^{\infty}(-1)^{m-1}\frac{q^{(2m-1)/2}}{1-q^{(2m-1)/2}}.\end{aligned}$$

定理 9.22 (Jacobi)

(1) 对于 $n \geqslant 1$ 有

$$r_4(n) = 8 \sum_{\substack{d|n \\ d \not\equiv 0 \mod 4}} d.$$

特别地, $r_4(n) \geqslant 8$.

(2)

$$\begin{aligned}\vartheta(z)^4 = \left(\sum_{n=-\infty}^{\infty} q^{n^2/2}\right)^4 &= 1 + 8\sum_{4 \nmid n} \frac{nq^{n/2}}{1-q^{n/2}} \\ &= 1 + 8\sum_{n=1}^{\infty} \frac{nq^{n/2}}{1-q^{n/2}} - 8\sum_{n=1}^{\infty} \frac{4nq^{2n}}{1-q^{2n}}.\end{aligned}$$

[证明] (2)⇒(1) 由

$$1 + 8\sum_{4\nmid d} \frac{dq^{d/2}}{1-q^{d/2}} = 1 + 8\sum_{4\nmid d}\sum_{m=1}^{\infty} dq^{dm/2} = 1 + 8\sum_{n=1}^{\infty}\left(\sum_{\substack{d|n \\ 4\nmid 4}} d\right) q^{n/2}$$

得知. (2) 的证明方法是看出两端都是权 2 的自守形式导出相等. 例如, 对于

$$F(z) = \frac{\vartheta(z)^4 - \left(1 + 8\sum_{4\nmid n} \dfrac{nq^{n/2}}{1-q^{n/2}}\right)}{\eta(z)^4},$$

$|F(z)|$ 关于

$$\Gamma = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \subset SL_2(\mathbb{Z})$$

不变的断言, 只要指出在所有的尖点 (这里是 3 个) 处其为 0 即可, 我们在此就不证明了. 现在我们来介绍 Ramanujan(1916年) 所考虑过的 "初等的" 方法 (所得到的等式是属于椭圆函数论范畴的). 由于有前面的 $(*)$, 我们只要证明

$$(**) \qquad \left(1 + 4\sum_{m=1}^{\infty} (-1)^{m-1} \frac{q^{(2m-1)/2}}{1-q^{(2m-1)/2}}\right)^2 = 1 + 8\sum_{4\nmid n} \frac{nq^{n/2}}{1-q^{n/2}}$$

即可. 为简单起见, 令

$$u_r = \frac{q^{r/2}}{1-q^{n/2}},$$

我们考虑对于实数 θ 的

$$\begin{aligned}S(\theta) &= \frac{1}{4}\cot\frac{\theta}{2} + u_1 \sin\theta + u_2 \sin 2\theta + \cdots, \\ T_1(\theta) &= \left(\frac{1}{4}\cot\frac{\theta}{2}\right)^2 + u_1(1+u_1)\cos\theta + u_2(1+u_2)\cos 2\theta + \cdots, \\ T_2(\theta) &= \frac{1}{2}\{u_1(1-\cos\theta) + 2u_2(1-\cos 2\theta) + 3u_3(1-\cos 3\theta) + \cdots\}.\end{aligned}$$

此时, 成立以下的

$$(***)\qquad S(\theta)^2 = T_1(\theta) + T_2(\theta).$$

后面我们再转回来证明它. 现在在 $(***)$ 中令 $\theta = \dfrac{\pi}{2}$, 我们来看看怎么得到前面的 $(**)$:

$$\begin{aligned}
S\left(\frac{\pi}{2}\right) &= \frac{1}{4} + u_1 - u_3 + u_5 - u_7 + \cdots,\\
T_1\left(\frac{\pi}{2}\right) &= \frac{1}{16} + \sum_{m=1}^{\infty}(-1)^m u_{2m}(1+u_{2m})\\
&= \frac{1}{16} + \sum_{m=1}^{\infty}(-1)^m \frac{q^m}{(1-q^m)^2}\\
&= \frac{1}{16} + \sum_{m=1}^{\infty}(-1)^m \sum_{n=1}^{\infty} n q^{mn}\\
&= \frac{1}{16} - \sum_{n=1}^{\infty} \frac{nq^n}{1+q^n}\\
&= \frac{1}{16} - \sum_{n=1}^{\infty}\left(\frac{nq^n}{1-q^n} - \frac{2nq^{2n}}{1-q^{2n}}\right)\\
&= \frac{1}{16} - \sum_{n:\text{奇数}} n u_{2n}\\
T_2\left(\frac{\pi}{2}\right) &= \frac{1}{2}(u_1 + 3u_3 + 5u_5 + \cdots) + 2(1\cdot u_2 + 3\cdot u_6 + 5\cdot u_{10} + \cdots),
\end{aligned}$$

由此得到了 $(**)$.

再来证明 $(***)$. 令

$$\begin{aligned}
S(\theta)^2 &= \left(\frac{1}{4}\cot\frac{\theta}{2}\right)^2 + \frac{1}{2}\cot\frac{\theta}{2}\sum_{m=1}^{\infty} u_m \sin m\theta + \left(\sum_{m=1}^{\infty} u_m \sin m\theta\right)^2\\
&= \left(\frac{1}{4}\cot\frac{\theta}{2}\right)^2 + S_1(\theta) + S_2(\theta),
\end{aligned}$$

$$S_1(\theta) = \frac{1}{2}\cot\frac{\theta}{2}\sum_{m=1}^{\infty} u_m \sin m\theta,$$

这里利用三角函数的积化和差公式

$$\cot\frac{\theta}{2}\sin m\theta = 1 + 2\cos\theta + 2\cos 2\theta + \cdots + 2\cos(m-1)\theta + \cos m\theta,$$

故而可写为

$$S_1(\theta) = \sum_{m=1}^{\infty}\left\{\frac{1}{2} + \cos\theta + \cos 2\theta + \cdots + \cos(m-1)\theta + \frac{1}{2}\cos m\theta\right\} u_m,$$

而

$$\begin{aligned}S_2(\theta) &= \sum_{m,n=1}^{\infty} u_m u_n \sin m\theta \sin n\theta \\ &= \frac{1}{2}\sum_{m,n=1}^{\infty} u_m u_n \{\cos(m-n)\theta - \cos(m+n)\theta\}.\end{aligned}$$

因此合起来有

$$S_1(\theta) + S_2(\theta) = \sum_{k=0}^{\infty} C_k \cos k\theta,$$

并且

$$\begin{aligned}C_0 &= \left(\frac{1}{2}\sum_{m=1}^{\infty} u_m\right) + \left(\frac{1}{2}\sum_{m=1}^{\infty} u_m^2\right) = \frac{1}{2}\sum_{m=1}^{\infty} u_m(1+u_m) \\ &= \frac{1}{2}\sum_{m=1}^{\infty} \frac{q^{m/2}}{(1-q^{m/2})^2} = \frac{1}{2}\sum_{m,n=1}^{\infty} nq^{mn/2} \\ &= \frac{1}{2}\sum_{n=1}^{\infty} \frac{nq^{n/2}}{1-q^{n/2}} = \frac{1}{2}\sum_{n=1}^{\infty} nu_n.\end{aligned}$$

对于 $k \geqslant 1$ 有

$$\begin{aligned}C_k &= \left(\frac{1}{2}u_k + \sum_{m=k+1}^{\infty} u_m\right) \\ &\quad + \left(\frac{1}{2}\sum_{m-n=k} u_m u_n + \frac{1}{2}\sum_{n-m=k}^{\infty} u_m u_n - \frac{1}{2}\sum_{m+n=k} u_m u_n\right) \\ &= \frac{1}{2}u_k + \sum_{l=1}^{\infty} u_{k+l} \sum_{l=1}^{\infty} u_l u_{k+l} - \frac{1}{2}\sum_{l=1}^{k-1} u_l u_{k-l},\end{aligned}$$

那么利用

$$\begin{aligned}&u_{k+l} + u_l u_{k+l} = u_{k+l}(1+u_l) = u_k(u_l - u_{k+l}), \\ &u_k u_{k-l} = u_k(1 + u_l + u_{k-l})\end{aligned}$$

我们得到

$$\begin{aligned}C_k &= u_k\left\{\frac{1}{2} + \sum_{l=1}^{\infty}(u_l - u_{k+l}) - \frac{1}{2}\sum_{l=1}^{k-1}(1 + u_l + u_{k-l})\right\} \\ &= u_k\left\{\frac{1}{2} + u_1 + \cdots + u_k - \frac{1}{2}(k-1) - (u_1 + u_2 + \cdots + u_{k-1})\right\} \\ &= u_k\left(1 + u_k - \frac{k}{2}\right).\end{aligned}$$

因此成立

$$
\begin{aligned}
S(\theta)^2 &= \left(\frac{1}{4}\cot\frac{\theta}{2}\right)^2 + \frac{1}{2}\sum_{n=1}^{\infty} n u_n + \sum_{k=1}^{\infty} u_k\left(1 + u_k - \frac{k}{2}\right)\cos k\theta \\
&= \left(\frac{1}{4}\cot\frac{\theta}{2}\right)^2 + \sum_{m=1}^{\infty} u_m(1+u_m)\cos m\theta + \frac{1}{2}\sum_{m=1}^{\infty} m u_m(1-\cos m\theta) \\
&= T_1(\theta) + T_2(\theta).
\end{aligned}
$$

证毕. ∎

(b) Siegel 自守形式

我们来介绍作为多元自守形式代表性例子的 **Siegel 自守形式** (Siegel modular form). 对于自然数 $n \geqslant 1$, n 次 **Siegel 模群** (Siegel modular group)

$$
\Gamma_n = Sp_n(\mathbb{Z}) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_{2n}(\mathbb{Z}) \,\middle|\, \begin{matrix} {}^tAC = {}^tCA,\ {}^tBD = {}^tDB, \\ {}^tAD - {}^tCB = I_n \end{matrix} \right\}
$$

为有限生成群, 定义它在 n 次 **Siegel 上半空间** (Siegel upper half space) $\left(复\ \dfrac{n(n+1)}{2}\right.$ 维空间$\left.\right)$

$$
H_n = \{Z \in M_n(\mathbb{C}) \mid {}^tZ = Z,\ \mathrm{Im}Z\text{为正定}\}
$$

的作用为

$$
\begin{array}{ccc}
H_n & \longrightarrow & H_n \\
\Psi & & \Psi \\
Z & \longmapsto & (AZ+B)(CZ+D)^{-1}
\end{array}
$$

(其中, $\mathrm{Im}Z$ 表示 Z 的虚数部分). $n=1$ 时, $\Gamma_1 = SL_2(\mathbb{Z})$, $H_1 = H$ 成为通常的情形. 再者, Γ_n 的条件, 当令

$$
J_n = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}
$$

时可写为

$$
\Gamma_n = \{M \in M_{2n}(\mathbb{Z}) \mid {}^tMJ_nM = J_n\} \subset SL_{2n}(\mathbb{Z}).
$$

还有, 对于一般的环 R,

$$
Sp_n(R) = \{M \in M_{2n}(R) \mid {}^tMJ_nM = J_n\}.
$$

权 k 的全纯自守形式的空间, 对于 $n \geqslant 2$ 为

$$
M_k(\Gamma_n) = \left\{ f : H_n \to \mathbb{C}\text{全纯} \,\middle|\, \begin{matrix} f((AZ+B)(CZ+D)^{-1}) = \det(CZ+D)^k f(Z) \\ \text{对于所有的} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n \text{ 成立.} \end{matrix} \right\}
$$

当 $n \geqslant 2$ 时, 在尖点 "$i\infty$" 的全纯性条件是自动出现的, 这便是说 "Koecher 原理" 成立. 自守性条件成为了对于 Γ_n 的有限个生成元的条件. 另外, 尖点形式构成的子空间定义为(对于 $n \geqslant 2$)

$$S_k(\Gamma_n) = \mathrm{Ker}(\Phi : M_k(\Gamma_n) \to M_k(\Gamma_{n-1})),$$

$$(\Phi f)(Z') = \lim_{t\to+\infty} f\begin{pmatrix} & & 0 \\ & Z' & \vdots \\ & & 0 \\ 0 & \cdots 0 & it \end{pmatrix}$$

(若看作 $M_k(\Gamma_0) = \mathbb{C}$, 则对 $n = 1$ 也同样成立). 这些 $M_k(\Gamma_n)$, $S_k(\Gamma_n)$ 全都是有限维的向量空间.

这里还有由 Maass(1951年) 构建的 Hecke 算子 $T(m)$ 的理论, 对于作为特征函数 $f \in M_k(\Gamma_n)$ 的基本 L 函数

$$L(s,f) = \prod_p H_p(p^{-s}, f)^{-1}$$

是 2^n 次的 Euler 积, 这里

$$H_p(u,f) = 1 - \lambda(p,f)u + \cdots + p^{2^{n-1}(nk - \frac{n(n+1)}{2})}u^{2^n},$$

其中, $\lambda(m,f)$ 为 $T(m)$ 的特征值: $T(m)f = \lambda(m,f)f$.

一般地, 有猜想: "$L(s,f)$ 在全平面为亚纯函数并且具有 $s \leftrightarrow n\left(k - \dfrac{n+1}{2}\right) + 1 - s$ 这样的函数方程". 在 f 不是尖点形式时, 根据关系式

$$L(s,f) = L(s,\Phi f)L(s-k+n,\Phi f),$$

它归结到 $n-1$ 次的元 $\Phi f \in M_k(\Gamma_{n-1})$, 故而只要考虑尖点的情形就可以了. 当 $n=1$ 时 $L(s,f)$ 为 §9.6 中的 L 函数, 从而已知. 当 $n=2$ 时的情形由 Andrianov(1974年) (基本上) 解决. 在 $n \geqslant 3$ 且 f 为尖点形式时还不能证明 f 的解析性.

我们来看一下次数为 2 的情形. 此时有

$$H_p(u,f) = 1 - \lambda(p,f)u + (\lambda(p,f)^2 - \lambda(p^2,f) - p^{2k-4})u^2 - p^{2k-3}\lambda(p,f)u^3 + p^{4k-6}u^4,$$

于是 $L(s,f)$ 是被解析延拓为整个 s 平面上的亚纯函数, 并具有函数方程

$$\widehat{L}(s,f) = (-1)^k \widehat{L}(2k-2-s,f).$$

而

$$\widehat{L}(s,f) = \Gamma_{\mathbb{C}}(s)\Gamma_{\mathbb{C}}(s-k+2)L(s,f).$$

至于证明, 我们利用 $\widehat{L}(f,s)$ 是将 f 限制在 H_2 的实 3 次元的子空间 (同构于 $SL_2(\mathbb{C})/SU(2)$) 的积分变换. 再有, 对于 $f\in S_k(\Gamma_2)$ 也有猜想

"$L(s,f)$ 为全纯, 并满足类比的 Ramanujan 猜想

$$H_p(u,f)=(1-\alpha u)(1-\beta u)(1-\gamma u)(1-\delta u) \text{ 时},$$
$$|\alpha|=|\beta|=|\gamma|=|\delta|=p^{k-\frac{3}{2}}\text{''},$$

已知有对此猜想的反例. 例如, $S_{10}(\Gamma_2)$ 是个 1 次元, 对于它的元 χ_{10} 有

$$L(s,\chi_{10})=\zeta(s-8)\zeta(s-9)L(s,\Delta E_6).$$

这里的 ΔE_6 是 $S_{18}(\Gamma_1)$ (一次元) 的元. 因此, $L(s,\chi_{10})$ 在 $s=10$ 具有了一阶的极点, 特别有了

$$H_p(u,\chi_{10})=(1-p^8u)(1-p^9u)(1-\gamma u)(1-\delta u)$$

(因为 ΔE_6 满足 Ramanujan 猜想, 故有 $|\gamma|=|\delta|=p^{\frac{17}{2}}$). 于是, 不满足这个类比的 Ramanujan 猜想. 这样的 "例外" 可以理解为它是由关于 $\Gamma_1=SL_2(\mathbb{Z})$ 的权 $2k-2$ 的自守形式而来的 (现在情形的 χ_{10} 来自 ΔE_6). $n=2$ 时我们已知有 Ramanujan 的同余式

$$\lambda(m,\Delta)\equiv\lambda(m,E_{12}) \mod 691$$

的类比.

例如, 有权 10 的尖点形式 χ_{10} 与 Eisenstein 级数 φ_{10} 的同余式

$$\lambda(m,\chi_{10})\equiv\lambda(m,\varphi_{10}) \mod 43867,$$

以及权 20 的 (第 3) 尖点形式 $\chi_{20}^{(3)}$ 与 Eisenstein 级数 $[\Delta E_8]$(这是由 $\Delta E_8\in S_{20}(\Gamma_1)$ 构成的 Eisenstein 级数) 的同余式

$$\lambda\left(m,\chi_{20}^{(3)}\right)\equiv\lambda(m,[\Delta E_8]) \mod 71^2$$

等等. 然而, 前一个由 Γ_1 的权 18 的自守形式之间的同余式

$$\lambda(m,\Delta E_6)\equiv\lambda(m,E_{18}) \mod 43867$$

所传承 (43867 是 Bernoulli 数 B_{18} 的分子, 即 $\zeta(18)$ 的代数部分的分子, 这才是本质所在). 还有, 后者的同余式的背景在于, 与 Ramanujan 的同余式中 691 起源于 $\zeta(12)$ 代数部分的分子 (B_{12} 的分子)(参考 §10.3(e)) 一样, 71^2 为 $L(38,\mathrm{Sym}^2(\Delta E_8))$ 的代数部分的分子. 这样一来, 自守形式之间的同余与 ζ 的特定值深深地联系在一起了.

对于一般的次数 $n\geqslant 3$ 的情形, L 函数的性质是对于自守形式以及自守表现 (的关联性) 的 Langlands 猜想的一个环节, 然而情况仍旧不明朗. 在 Siegel 自守形式的情形, 对于实解析的自守形式与它的 L 函数的理论也仍然在进行着研究.

小结

9.1　自守形式的自守性是个很强的条件, 而自守形式具有漂亮的性质. 在很多场合全纯的自守形式之间都存在着代数关系.

9.2　由自守形式可构造 ζ, 并具有函数方程. 这些函数方程就是自守性的另一种的说法, 并且有某一类似的函数方程可以反过来推导出自守性. 因此, 自守形式与 ζ 之间存在着 "1-1 对应".

9.3　自守形式中的 Eisenstein 级数以及 Ramanujan 的 Δ 是特别基本的, 可以得到与其相关的各种各样的有深刻意义的等式.

9.4　自守形式中除了全纯的外还有实解析的. 特别地, 实解析的 Eisenstein 级数在 Kronecker 极限公式等方面有着广泛的应用.

习题

9.1　证明下面的等式, 其中 $n \geqslant 1$ 为整数.

(1) $\sigma_7(n) = \sigma_3(n) + 120 \sum\limits_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)$.

(2) $11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum\limits_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m)$.

(3) $36\tau(n) = 5\sigma_3(n) + 10\sigma_7(n) + 21\sigma_5(n)$

$$+2400 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_7(n-m) - 5292 \sum_{m=1}^{n-1} \sigma_5(m)\sigma_5(n-m).$$

9.2　当 $k \geqslant 6$ 满足 $k \equiv 2 \mod 4$ 时, 求

$$\sum_{n=1}^{\infty} \frac{n^{k-1}}{e^{2\pi n} - 1}.$$

9.3　证明下面的等式. 其中

$$\varpi = 2\int_0^1 \frac{dx}{\sqrt{1-x^4}}$$

为双纽线周率.

(1) $\sum\limits_{n=1}^{\infty} \dfrac{1}{n(e^{2\pi n}-1)} = -\dfrac{\pi}{12} - \frac{1}{2}\log\left(\dfrac{\varpi}{\sqrt{2}\pi}\right)$.

(2) $\sum\limits_{m,n=-\infty}^{\infty}{}' \dfrac{1}{(m+ni)^8} = \dfrac{\varpi^8}{525}$.

(3) $\sum\limits_{m,n=-\infty}^{\infty}{}' \dfrac{1}{(m+ni)^{12}} = \dfrac{2\varpi^{12}}{53625}$.

9.4

(1) 设 $\rho = \dfrac{-1+\sqrt{3}i}{2}$, 证明 $E_4(\rho) = 0,\ E_6(\rho) \neq 0$.

(2) 对于 $k=2,4,8$ 求

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}n^{k-1}}{e^{\sqrt{3}\pi n}+(-1)^{n-1}}.$$

9.5 证明下面的四个性质等价.

(i) 对于所有的素数 p, $|\tau(p)|\leqslant 2p^{\frac{11}{2}}$ 成立 (Ramanujan 猜想).

(ii) 对于所有的素数 p, 存在 (唯一的)$0\leqslant\theta_p\leqslant\pi$ 使得 $\tau(p)=2p^{\frac{11}{2}}\cos\theta_p$.

(iii) 对于所有的自然数 n, 成立 $|\tau(n)|\leqslant n^{\frac{11}{2}}d(n)$.

(iv) 对于任意的 $\varepsilon>0$ 成立 $\tau(n)=O(n^{\frac{11}{2}+\varepsilon})$. (换句话说, 对于任意 ε, $\dfrac{\tau(n)}{n^{\frac{11}{2}+\varepsilon}}$ 有界.)

9.6 对于数域 K, 求以下的值.

(1) Dedekind ζ 函数 $\zeta_K(s)$ 在 0 的微分 $\zeta_K'(0)$.

(2) K 的非零整理想 $\boldsymbol{a}$ 的范 $N(\boldsymbol{a})$ 的正规积 $\prod\limits_{\boldsymbol{a}}N(\boldsymbol{a})$.

第十章 岩泽理论

我们在本章将对岩泽理论进行概要性讲解. 在第三章中所叙述的第二个和第三个奇特性质将在本章的岩泽理论中得到升华. 关于 ζ 函数、L 函数的重要性至今也已以各种各样的方式叙述过, 在这里我们还要举出 ζ 函数的 p 进方面的特性. 在研究 Kummer 的分圆域时, ζ 的 p 进的一面可以说仅仅是一点点窥视而已 (第二个奇特性质, 参看 §3.3(e)), 然而最早捕捉住它, 将其作为 p 进连续函数的性态的是 20世纪60 年代的久保田 (Kubota)–Leopoldt. 岩泽健吉则发现了这个 p 进 L 函数附着于 Galois 群的群环之上, 进一步他提出了下面这个称之为**岩泽主猜想** (Iwasawa main conjecture) 的关系式:

$$(\text{解析的 } p \text{ 进 } \zeta) = (\text{代数的 } p \text{ 进 } \zeta)$$

在这里, 左端的解析 p 进 ζ 是说, 它是按照 ζ 函数值的 p 进性质, 在 p 进世界中以 p 进解析定义的函数. 而右端的代数 p 进 ζ 可以表述为关于理想类群的某个线性映射的行列式, 是个以代数方式定义的对象. 在 ζ 函数理论中, 寻求其行列式表示是一个重要问题 (参照 §9.5(c)), 然而现在, 如果能由上面等式左端的解析 p 进 ζ 来观察的话, 意味着得到了它的行列式表示, 从而 L 函数的值的 p 进性质的研究取得了很大的进展. 反过来说, 从此等式右端的代数 p 进一侧来看, 则意味着解析的 p 进 ζ 告诉了我们关于理想类群的数论中想要知道而又难于了解的对象的信息. 这样的岩泽理论是 (p 进) 解析对象与数论对象之间的深刻而漂亮的理论.

由于篇幅的缘故, 在本章中, 我们将尽量以形成岩泽理论核心的岩泽主猜想为焦点进行讲解.

岩泽健吉所提出的这个猜想的关系式在 1984 年由 Mazur 和 Wiles(更为一般的情形由 Wiles 在 1990年) 解决. 另外, 一进入 20世纪90年代, Rubin, Greither 使用

由 Kolyvagin 所引进的 Euler 系的概念, 成功地给出了对它的全新证明. 他们的证明的思想将在 §10.3 中稍有谈及.

我们在 §10.0 中对岩泽理论作初步介绍之后, 接着便在 §10.1 中研究了前面所说的解析 p 进 ζ, 而后在 §10.2 中则处理了上面提到的代数的 p 进 ζ. 这里的主要角色是理想类群. 我们在 §10.3 中则给出这两者之间关系的岩泽主猜想的正式表述, 并讲述了它的应用.

§10.0 何谓岩泽理论

岩泽理论是研究 ζ 函数值的 p 进性质与理想类群的 p 进性质之间关系的理论. 在 §10.0 中将叙述根据岩泽理论我们到底能了解哪些事, 以及要如何做才算可以被看成是岩泽理论的理论. 在这里我们以理想类群为中心进行叙述.

(a) 分圆域的理想类群

我们首先从岩泽理论的 "出生地" 分圆域说起. 对于正整数 $n > 0$, 以 μ_n 表示有理数域 $\mathbb{Q}$ 的代数闭包 $\overline{\mathbb{Q}}$ 中的 n 次单位根所构成的群, 以 $\mathbb{Q}(\mu_n)$ 表示在 $\mathbb{Q}$ 中添加 μ_n 的所有元所得到的域. 设 $\zeta_n \in \mu_n$ 为 n 次本原单位根, 于是有 $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$.

如在 §4.4(b) 中叙述过的那样, Kummer 在 19 世纪中叶发现了现在称之为 Kummer 判别法的, 关于 ζ 函数值与理想类群之间的令人惊奇的关系. 对于素数 p, 记分圆域 $\mathbb{Q}(\mu_p)$ 的理想类群 $Cl(\mathbb{Q}(\mu_p))$ 的阶数为 $h_{\mathbb{Q}(\mu_p)}$, 并断言

$$p | h_{\mathbb{Q}(\mu_p)} = \# Cl(\mathbb{Q}(\mu_p))$$

$$\text{与 } p \text{ 除尽 } \zeta(-1), \zeta(-3), \zeta(-5), \cdots, \text{中一个的分子}$$

等价. 在这里, $\zeta(s)$ 为 Riemann ζ 函数, 是将 $\sum\limits_{n=1}^{\infty} \dfrac{1}{n^s}$ 解析延拓到整个 $\mathbb{C}$ 平面得到的函数.

称满足上面等价条件的素数 p 为**非正则素数** (irregular prime). 在第四章曾说过, 691 是个非正则素数. 非正则素数按大小顺序连续排列为

$$37, 59, 67, 101, \cdots,$$

并已知有无限多个. (称不是非正则素数的素数为**正则素数**(regular prime)).

那么, 我们举出最小的非正则素数来看. 按照上面的 Kummer 判别法, $h_{\mathbb{Q}(\mu_{37})}$ 被 37 除尽, 然而实际上我们已知 $h_{\mathbb{Q}(\mu_{37})} = 37$. 因此, 理想类群 $Cl(\mathbb{Q}(\mu_{37}))$ 为 37 阶的循环群. 在此, 如果依照岩泽理论, 则可得到更为详细的信息. 设 $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_{37})/\mathbb{Q})$ 为 $\mathbb{Q}(\mu_{37})/\mathbb{Q}$ 的 Galois 群. 像在 §5.2 中所叙述的那样, 有自然同构 $\omega : \Delta \xrightarrow{\sim} (\mathbb{Z}/37)^\times$. 于是我们有了被记为 ω 的这个同构. Δ 自然地作用于 $Cl(\mathbb{Q}(\mu_{37}))$ 上. (对于 $\sigma \in \Delta$ 与 $x = [\boldsymbol{a}] \in Cl(\mathbb{Q}(\mu_{37}))$, 作用为 $\sigma(x) = [\sigma(\boldsymbol{a})]$.) 岩泽理论会告诉我们这个作用是什么样的. 也就是说, 对于 $x \in Cl(\mathbb{Q}(\mu_{37}))$ 和 $\sigma \in \Delta$, 按照岩泽理论我们将知道有

$$\sigma(x) = \omega(\sigma)^5 \cdot x. \tag{10.1}$$

于是, 岩泽理论描述了仅像类数公式之类的范围内不能了解的群的作用情形. 下面的 (b) 小节中我们将叙述由什么样的理论推导出了 (10.1).

(b) Herbrand, Ribet 的定理

对于在 (a) 小节中所叙述的 Galois 群的作用, 我们来更详细地加以阐述. 设 p 为奇素数, $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ 为扩域 $\mathbb{Q}(\mu_p)/\mathbb{Q}$ 的 Galois 群, $\omega : \Delta \xrightarrow{\sim} (\mathbb{Z}/p)^\times$ 为自然同构. 此时, 关于 ζ 函数值与 $\mathbb{Q}(\mu_p)$ 的理想类群的关系, 我们有比 Kummer 判别法更为详细的下面的定理.

定理 10.1 (Herbrand, Ribet) *对于正偶数 r, 以下条件等价:*

(1) p 除尽 $\zeta(1-r)$ 的分子.

(2) 在理想类群 $Cl(\mathbb{Q}(\mu_p))$ 中的 p 阶元 x, 对于任意 $\sigma \in \Delta$ 成立

$$\sigma(x) = \omega(\sigma)^{1-r}x.$$ □

由 (2) 推出 (1) 是由 Herbrand 在 1930 年得到的, 而由 (1) 推出 (2) 则是在较晚的 1976 年由 Ribet 证明的. Ribet 的证明使用了自守形式, 我们将在 §10.3(e) 中给出他的证明思想. 这一章的目的是由岩泽主猜想直接地推导出这个定理. 我们将在 §10.3(c) 中予以叙述.

那么, 由于 37 除尽了 $\zeta(-31)$ 的分子 (参看 §10.1(a)), 并注意到 Δ 的阶数为 36, 于是由上面的定理 10.1 知道存在下述事实, 对于 37 阶元 x 满足 $\sigma(x) = \omega(\sigma)^{-31}x = \omega(\sigma)^5x$, 于是得到了 (a) 小节的 (10.1) 式.

这个岩泽理论是最早写出来的研究 ζ 函数值的 p 进性质与理想类群的 p 进性质间的深刻关系的理论. 我们将至此所叙述的有关事实列表于后.

表 10.1 ζ 函数的 p 进性质所对应的理想类群的性质

	ζ 函数的 p 进性质	理想类群
Kummer 判别法	p 为除尽 $\zeta(-1), \zeta(-3), \zeta(-5), \cdots$ 的某个分子	p 除尽 $Cl(\mathbb{Q}(\mu_p))$ 的阶数
Herbrand, Ribet 的定理 (由岩泽主猜想直接推出)	p 除尽 $\zeta(1-r)$ 的分子, 其中 r 为正偶数	$Cl(\mathbb{Q}(\mu_p))$ 的 p 阶元 x, $\sigma(x) = \omega(\sigma)^{1-r}x\,(\sigma \in \Delta)$ 成立 (r 为正偶数)
对于 $p = 37$	$p \mid \zeta(-31)$	$\sigma(x) = \omega(\sigma)^5x$ $(x \in Cl(\mathbb{Q}(\mu_p)), \sigma \in \Delta)$

(c) $K(\mu_{p^n})$ 的理想类群

对于数域, 即有理数域 $\mathbb{Q}$ 的有限扩域 K, 岩泽理论将 $K(\mu_{p^n})$ 的理想类群的性状以统一的方式告诉了我们. 在下面我们固定一个素数 p, 对于任意数域 F, 被 p 幂零化的 $Cl(F)$ 的所有元构成的子群记为 A_F. A_F 为 $Cl(F)$ 的 p-Sylow 群. 譬如, 对

于 $p=37$, $Cl(\mathbb{Q}(\mu_{37}))=A_{\mathbb{Q}(\mu_{37})}\simeq\mathbb{Z}/37$. 如果使用岩泽理论, 则进一步对于添加 1 的 37^n 幂根得到的域 $\mathbb{Q}(\mu_{37^n})$ (设 $p=37$), 可以证明

$$\begin{aligned} &A_{\mathbb{Q}(\mu_{37})}\simeq\mathbb{Z}/37\\ &A_{\mathbb{Q}(\mu_{37^2})}\simeq\mathbb{Z}/37^2\\ &\quad\vdots\\ &A_{\mathbb{Q}(\mu_{37^n})}\simeq\mathbb{Z}/37^n.\qquad(n\geqslant1)\end{aligned}$$

在证明这个断言时, 成为关键点的 ζ 函数值的 p 进性质列在下面的表 10.2 中 (关于证明参考问题 6 及习题 10.2).

表 10.2　按照岩泽理论, 在计算理想类群时成为关键点的 ζ 函数值的性质

ζ 函数的p 进性质	理想类群
$37\mid\zeta(-31)$	$A_{\mathbb{Q}(\mu_{37})}\neq0$
$67\zeta(-31)\not\equiv31\zeta(-67)\pmod{37^2}$	$A_{\mathbb{Q}(\mu_{37})}\simeq\mathbb{Z}/37$
$\zeta(-31)\not\equiv\zeta(-67)\pmod{37^2}$	$A_{\mathbb{Q}(\mu_{37^n})}\simeq\mathbb{Z}/37^n\ (n\geqslant2)$

同样地, 对于 $p=691$ 也可证明有

$$\begin{aligned} &A_{\mathbb{Q}(\mu_{691})}\simeq\mathbb{Z}/691\oplus\mathbb{Z}/691\\ &\quad\vdots\\ &A_{\mathbb{Q}(\mu_{691^n})}\simeq\mathbb{Z}/691^n\oplus\mathbb{Z}/691^n\qquad(n\geqslant1).\end{aligned}$$

这时的关键点是, 691 不仅是 $\zeta(-11)$ 的分子, 而且除尽 $\zeta(-199)$ 的分子. 我们再举几个 $K\neq\mathbb{Q}$ 的例子. 我们能作如下的计算:

对于 $K=\mathbb{Q}(\sqrt{-31})$, $p=3$,

$$\begin{aligned} &A_{K(\mu_3)}\simeq\mathbb{Z}/3\\ &A_{K(\mu_9)}\simeq\mathbb{Z}/9\\ &\quad\vdots\\ &A_{K(\mu_{3^n})}\simeq\mathbb{Z}/3^n\qquad(n\geqslant1)\end{aligned}$$

对于 $K=\mathbb{Q}(\sqrt{-1399})$, $p=3$,

$$\begin{aligned} &A_{K(\mu_3)}\simeq\mathbb{Z}/27\\ &A_{K(\mu_9)}\simeq\mathbb{Z}/81\oplus\mathbb{Z}/3\\ &\quad\vdots\\ &A_{K(\mu_{3^n})}\simeq\mathbb{Z}/3^{n+2}\oplus\mathbb{Z}/3^{n-1}\qquad(n\geqslant1)\end{aligned}$$

对于 $K=\mathbb{Q}(\sqrt{-762})$, $p=3$,

$$\begin{aligned}
A_{K(\mu_3)} &\simeq \mathbb{Z}/3\oplus\mathbb{Z}/3\\
A_{K(\mu_9)} &\simeq \mathbb{Z}/9\oplus\mathbb{Z}/9\\
&\vdots\\
A_{K(\mu_{243})} &\simeq \mathbb{Z}/243\oplus\mathbb{Z}/243\\
A_{K(\mu_{729})} &\simeq \mathbb{Z}/729\oplus\mathbb{Z}/243\\
&\vdots\\
A_{K(\mu_{3^n})} &\simeq \mathbb{Z}/3^n\oplus\mathbb{Z}/243 \qquad (n\geqslant 5).
\end{aligned}$$

进一步说, 在 $A_{K(\mu_{p^n})}$ 上 $K(\mu_{p^n})/K$ 的 Galois 群 $\mathrm{Gal}(K(\mu_{p^n})/K)$ 如何作用, 尽管也为岩泽理论所记述, 但关于此类则要在 §10.2 之后方可看到.

一般地, 对于任意的数域 K, 令 $K_n=K(\mu_{p^n})$, 关于 A_{K_n} 的阶数, 岩泽证明 (1959 年) 对于充分大的所有 n, 存在满足

$$\#A_{K_n}=p^{\lambda n+p^n\mu+\nu} \quad (n\gg 0)$$

的常数 λ, μ, ν (参照 §10.2(f)). 这可以说成是岩泽理论的起点. 为什么要考虑理想类群的 p-Sylow 群呢? 为什么要考虑形如 $K(\mu_{p^n})$ 的域呢? 有关于此, 请参考下面的 (d) 和 (e) 小节.

我们把到此为止已写的东西小结一下.

1. 岩泽理论是处理 ζ 函数值的 p 进性质与理想类群的 p 进性质间所存在的深刻关系的理论.
2. 岩泽理论描述了 Galois 群对理想类群作用.
3. 岩泽理论统一地描述了 $K(\mu_{p^n})$ 的理想类群的 p-Sylow 子群.

(d) 数域与函数域的类似

在此 (d) 小节与后面的 (e) 小节中, 我们将叙述岩泽主猜想是如何产生的, 以及岩泽理论创始人岩泽健吉的想法. 对于想要进一步了解的读者, 我们推荐注记中的文献①. 尽管其中有一些不懂的语句, 也不妨请边阅读边思考. 在 (e) 的最后面, 我们在一种特殊的情形下叙述了岩泽主猜想.

到现在为止, 理想类群多次出现, 表明它在数论中是起着非常重要作用的群. 它的微妙的结构对于数论问题而言包含了决定性的信息. 然而即便以二次域的类数表作为例子来看, 我们也几乎没有感到有任何规律性可言.

另一方面, 当考虑在函数域上的类比时, 有限域上代数曲线的次数为 0 的除子类群像在 §6.4(f) 中所讲的那样, 也是有限的 Abel 群, 它与理想类群一样也是个困难

①岩泽健吉, "关于数域与函数域的某些类似", 数学15(1963),65-67, 岩波书店.

的对象. 但是, 我们知道代数闭域上曲线的 0 次除子类群具有 Abel 簇的结构, 而这种情形是能够进行仔细研究的. 特别地, 当设 g 为曲线的亏格, 域的特征为 0 时, 它的扭元 (torsion) 部分同构于 $(\mathbb{Q}/\mathbb{Z})^{2g}$. 即便域的特征为正, 只要取 p 为不同于特征的素数, 那么扭元部分的 p 分支 (即被 p 幂化零的部分) 也同构于 $(\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$. 注意, 这里的 $\mathbb{Q}_p/\mathbb{Z}_p$ 为 $\mathbb{Q}/\mathbb{Z}$ 的 p 分支. 这样一来, 不同于理想类群, 代数闭域上曲线的 0 次除子类群具有只由亏格决定的简单形式.

有理数域 $\mathbb{Q}$ 的有限扩域 K 与有限域 $\mathbb{F}_q$ 上代数曲线 X 的函数域 $\mathbb{F}_q(X)$ 尽管说是类似的, 但将两者

$$K \qquad\qquad \mathbb{F}_q(X)$$
$$([K:\mathbb{Q}]<\infty)$$

进行比较, 其本质性不同点在于, 就 $\mathbb{F}_q(X)$ 而言, 有所谓的 "到代数闭域中去" 的处理方法, 就是说, 设 $\overline{\mathbb{F}_q}$ 为 $\mathbb{F}_q$ 的代数闭包, 则可考虑 $X\otimes_{\mathbb{F}_q}\overline{\mathbb{F}_q}$ 的函数域 $\overline{\mathbb{F}_q}(X)$. 那么, 举例来说, 通过自然映射 $Cl^0(\mathbb{F}_q(X))\to Cl^0(\overline{\mathbb{F}_q}(X))$, 可以研究 $Cl^0(\mathbb{F}_q(X))$. ($Cl^0(\mathbb{F}_q(X))$ 在 $Cl^0(\overline{\mathbb{F}_q}(X))$ 中的像包含在 $Cl^0(\overline{\mathbb{F}_q}(X))$ 的扭元部分中, 并注意到如上所说, 对于 $Cl^0(\overline{\mathbb{F}_q}(X))$ 的扭元部分能够有好的了解.) 岩泽因此考虑了如何才可以在数域上做出 $\overline{\mathbb{F}_q}(X)$ 的类比. 由于 $\overline{\mathbb{F}_q}$ 是由 $\mathbb{F}_q$ 添加了所有的单位根所得到的域, 那么, 在 K 中添加所有的单位根会是怎么样呢, 这种想法便首先出现了. 但是, 这样的域太大了, 会丢失相当多的关于理想类群的信息. 在这里, 当设 L 为 $\mathbb{Q}$ 的无限次代数扩域时, 我们定义 L 的理想类群 $Cl(L)$ 为群

$$Cl(L)=\varinjlim Cl(M)\quad (M \text{ 遍历 } L \text{ 中对于 } \mathbb{Q} \text{ 为有限次的子域}).$$

可是, 由于数域的理想类群 $Cl(K)$ 为有限 Abel 群,

$$Cl(K)=\bigoplus_{p:\text{素数}} Cl(K)\{p\}$$

可以分成对于各个素数的分支. 这里,

$$Cl(K)\{p\}=\{c\in Cl(K)\mid \text{存在某个 } m \text{ 使得 } p^m c=0\}.$$

如果对于所有的素数 p 已知 $Cl(K)\{p\}$, 则便可知 $Cl(K)$, 故我们在后面固定一个素数 p, 并从它的 p 分支着眼来进行研究. 在此, 固定一个素数 p, 对于 $\mathbb{Q}$ 的任意代数扩域 F, 以 A_F 表示 $Cl(F)\{p\}$.

那么, 如果只考察 A_F 而不添加所有的 p 幂单位根, 这样的想法可行吗? 以 μ_{p^n} 表示在 $\mathbb{Q}$ 的代数闭包 $\overline{\mathbb{Q}}$ 中的所有 p^n 次单位根形成的群, 对于数域 K, 以 $K(\mu_{p^n})$ 表示在 K 中添加所有 p^n 次单位根得到的域, 并定义 $K(\mu_{p^\infty})=\bigcup K(\mu_{p^n})$. 此时可以证明 $A_{K(\mu_{p^\infty})}$ 的结构能写成

$$A_{K(\mu_{p^\infty})}\simeq(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda\oplus\left[(\bigoplus^{\infty}A)/B\right].$$

其中 λ 为不小于 0 的整数, A 是阶为 p 幂的有限 Abel 群 (因此可写为 $A=\mathbb{Z}/p^{n_1}\oplus\cdots\oplus\mathbb{Z}/p^{n_r}$), $\bigoplus\limits^{\infty}A$ 为 A 的可数无限的直和, 而 B 为 $\bigoplus\limits^{\infty}A$ 的有限子群. 当 $K/\mathbb{Q}$ 为 Abel 扩域时, $\left(\bigoplus\limits^{\infty}A\right)/B$ 不出现, 于是知道有

$$A_{K(\mu_{p^\infty})}\simeq(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$$

(Ferrero-Washington 定理, 参看定理 10.9, 定理 10.32). 对于一般的 K, 有称为 "岩泽 $\mu=0$ 猜想" 的猜想, 它说此时也不会出现 $\bigoplus\limits^{\infty}A/B$ 项, 然而其在一般的情形并没有得到解决. 这样一来, 我们就可以知道, 如果考虑理想类群的 p 分支 (p-Sylow 群), 则 $K(\mu_{p^\infty})$ 便成了 $\overline{\mathbb{F}_q}(X)$ 的很好类比, 于是便可能有相似的结果. (可是还有遗留的问题, 例如这个整数 λ 是怎样的数?)

(e) Galois 群的作用

在 (a) 小节中我们已说过, 代数闭域上曲线的 0 次除子类群的扭元部分的 p 分支具有 $(\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$ 这样的结构. 这个事实除了作为 Abel 群其结构易于了解之外, 还有更为重要的意义. 现设 $\mathbb{F}_q$ 为特征不同于 p 的有限域, X 为 $\mathbb{F}_q$ 上的曲线, 考虑 $X\otimes_{\mathbb{F}_q}\overline{\mathbb{F}_q}$ 的除子类群, 在其上有 $\mathbb{F}_q$ 的 Frobenius 映射作用 (即 q 幂映射). 于是 Frobenius 映射也作用在 $Cl^0(\overline{\mathbb{F}_q}(X))\{p\}\simeq(\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$ 上, 从而给出了在 $(\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$ 上的同构映射, 于是这个作用可以用 $2g$ 阶矩阵 $A_X\in M_{2g}(\mathbb{Z}_p)$ 来表示. 这里的一个非常重要的事实是, 用 A_X 的特征多项式可以写出 X 的 ζ 函数 (称为同余 ζ). 这样在代数函数域的情形下, 根据对 Galois 群 $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ 的作用的考虑, 我们能得到非常重要的结果.

让我们回到数域的情形. 为简单计, 令 $K=\mathbb{Q}$. 在 (a) 小节曾说过有

$$A_{\mathbb{Q}(\mu_{p^\infty})}\simeq(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda.$$

Galois 群 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ 自然地作用在 $A_{\mathbb{Q}(\mu_{p^\infty})}$ 上. 这里, 因为 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ 与 $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)=\widehat{\mathbb{Z}}$ 不同且没有单个的生成元, 故在按照函数域的情形进行操作时, 一点也不另加考虑是不行的. 由于在 §5.2 中我们曾看到有自然同构 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})\xrightarrow{\sim}(\mathbb{Z}/p^n)^\times$, 故而可以构成自然同构

$$\kappa:\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})\xrightarrow{\sim}\mathbb{Z}_p^\times.$$

称这个映射为**分圆特征**, 并在此章中总以 κ 表示. 对于 $\sigma\in\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, $\kappa(\sigma)$ 对于任意的 $n>0$ 及任意的 $\zeta\in\mu_{p^n}$ 为满足 $\sigma(\zeta)=\zeta^{\kappa(\sigma)}$ 的元, 这是它的一个特征刻画. 在这里为简单起见我们假定 $p\neq2$ (在 §10.1 之后, 也处理一般的情形). 那么如在 §2.5 所见, 有 $\mathbb{Z}_p^\times\simeq(\mathbb{Z}/p)^\times\times(1+p\mathbb{Z}_p)$, 这里 $(\mathbb{Z}/p)^\times$ 为 $p-1$ 阶循环群, $1+p\mathbb{Z}_p$ 同构于加法群 $\mathbb{Z}_p$(参照 §10.1(b)). 取 $1+p\mathbb{Z}_p$ 的一个拓扑生成元 u. (就是说, 取一个使 $u-1$ 被 p 除尽, 而不被 p^2 除尽的元 u.) 而且设 $\gamma\in\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ 为使得满足

$\kappa(\gamma)=u$ 的元. 此时, 不禁冒出了这样的疑问: 如果与函数域的情形的类比有一点意义的话, 那么由 γ 在 $A_{\mathbb{Q}(\mu_{p^\infty})}$ 的作用所产生的特征多项式难道就与某个有某种意义的 ζ 函数没有任何关系吗? 令人非常吃惊, 真的非常吃惊, 回答竟是有关系. 由 γ 的作用便可得出久保田 –Leopoldt 的 p 进 L 函数. 所谓 p 进 L 函数是通过通常的 L 函数在整数处的值提炼出来的, 在 §10.1 将详细叙述这个函数.

对于上面所说的我们再稍加一点必要的说明. 定义同态 $\omega:\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})\to\mathbb{Z}_p^\times$ 为复合映射

$$\omega:\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})\xrightarrow[\kappa]{}\mathbb{Z}_p^\times\xrightarrow[\bmod p]{}(\mathbb{Z}/p)^\times\to(\mathbb{Z}/p)^\times\times(1+p\mathbb{Z}_p)\simeq\mathbb{Z}_p^\times$$
$$a\mapsto(a,1).$$

又定义 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ 的子群 Δ 为在同构 $\kappa:\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})\xrightarrow{\sim}\mathbb{Z}_p^\times=(\mathbb{Z}/p)^\times\times(1+p\mathbb{Z}_p)$ 下 $(\mathbb{Z}/p)^\times\times\{1\}$ 所对应的群. 对于满足 $0\leqslant i<p-1$ 的整数 i, 定义

$$A_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^i}=\{x\in A_{\mathbb{Q}(\mu_{p^\infty})}\mid \text{对所有的 }\sigma\in\Delta\text{ 有 }\sigma(x)=\omega(\sigma)^ix\},$$

又由 Δ 作用在模上的一般理论知, 存在分解

$$A_{\mathbb{Q}(\mu_{p^\infty})}=\bigoplus_{i=0}^{p-2}A_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^i}$$

(参看 §10.1 命题 10.12). 当记 $A_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^i}\simeq(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_i}$ 之后, 有 $\sum\limits_{i=0}^{p-2}\lambda_i=\lambda$. 那么, 因为 γ 作用在 $A_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^i}$ 上, 故 $\gamma-1$ 在 $A_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^i}\simeq(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_i}$ 的作用可以用矩阵 $A_i\in M_{\lambda_i}(\mathbb{Z}_p)$ (λ_i 阶矩阵) 表示. 记 A_i 的特征多项式为 $\varphi_i(T)\in\mathbb{Z}_p[T]$. 也就是说, $\varphi_i(T)=\det(TI-A_i)$.

这样所决定的多项式 $\varphi_i(T)$ 与可以说成是 Riemann ζ 函数的 p 进化身的 p 进 Riemann ζ 之间的关系: 这才是岩泽主猜想. 正如在本章一开头所说的, 由岩泽所猜测的这个漂亮的关系被 Mazur 和 Wiles 所证明. 在我们现在的情形, 成立下面的

定理 10.2 设 i 为满足 $1<i<p-1$ 的奇数.

(1) 对于满足$m\equiv i\pmod{p-1}$ 的任意**负整数** m, 存在唯一的幂级数 $g_i(T)\in\mathbb{Z}_p[[T]]$ 使得成立

$$g_i(u^m-1)=(1-p^{-m})\zeta(m).$$

其中, $\zeta(s)$ 为 Riemann ζ 函数, u 为上面所取的 $1+p\mathbb{Z}_p$ 的那个拓扑生成元. 函数

$$s\mapsto g_i(u^s-1)$$

是从 $\mathbb{Z}_p$ 到 $\mathbb{Z}_p$ 的 p 进连续函数, 这是由久保田–Leopoldt 发现的, 称之为 p 进 L 函数.

(2) (岩泽主猜想, Mazur-Wiles 定理) 上面所定义的特征多项式 $\varphi_i(T)$ 与 $g_i(T)$ 在 $\mathbb{Z}_p[[T]]$ 中仅相差一个可逆元. 这就是说, 他们生成同一个理想:

$$(\varphi_i(T)) = (g_i(T)).$$

■

于是, 由 $\gamma - 1$ 在 $A_{\mathbb{Q}(\mu_{p^\infty})}$ 上的作用, 我们能得出 Riemann ζ 函数的值! 在 §10.3 中我们将对于更一般的情形进行正式的系统阐述. 至于 $\mathbb{Q}(\mu_{p^\infty})$ 的理想类群, 我们将在 §10.3(b), (c) 中详细叙述.

§10.1 p 进解析 ζ

在此 §10.1 中我们要研究 ζ 函数值所具有的 p 进性质, 将看到存在被称做 p 进 L 函数的 "p 进全纯函数". 而且最后还要证明这个函数位于 Galois 群的群环之中.

(a) Riemann ζ 的特殊值: p 进世界的入口

ζ 函数具有 p 进性质这一点, 我们在 §3.3(e) 作为它的第二个奇特性质已经见到过了. 在这里将再次来观察这个性质.

设 $\zeta(s)$ 为 Riemann 的 ζ 函数, 即为在 $\mathrm{Re}(s) > 1$ 上函数 $\sum\limits_{n=1}^{\infty} \dfrac{1}{n^s}$ 解析延拓到整个 $\mathbb{C}$ 所得到的函数. 我们有 $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90, \cdots$, 而根据公式 $\zeta(2n) = \dfrac{2^{2n-1}}{(2n-1)!}|\zeta(1-2n)|\pi^{2n}$ (n为正整数) 知道, 考察在正偶数的值与考察在负奇数的值本质上是一样的.

那么, 我们在表 10.3 中写出 $\zeta(s)$ 在负奇数处的值来看看. 还有, 对于在负整数的值为有理数以及在负偶数的值为 0 的结论希望能参照 §3.3.

上面的值具有怎样的意义? 对于符号以及分母, 我们有下面的命题.

命题 10.3 设 $r > 0$ 为正偶数.

(1) 当 $\dfrac{r}{2}$ 为偶数时 $\zeta(1-r)$ 为正, 奇数时为负.

(2) 将 $\zeta(1-r)$ 写为既约分数时, 令其分母为 D_r, 则成立下面的断言:

(a) 对于任意素数 p, 有 p 除尽 D_r 的充分必要条件是 $p-1$ 除尽 r.

(b) 对于任意素数 p, 当 p 除尽 D_r 时, 有

$$\mathrm{ord}_p(D_r) = \mathrm{ord}_p(r) + 1.$$

□

根据 (2), 可以完全决定 $\zeta(1-r)$ 的分母 D_r. 读者可试着用表 10.3 来具体地确认 (2) 的正确性.

问题 1 利用命题 10.3 指出对于任意的 r, D_r 被 12 除尽.

上述(1) 可以, 譬如, 直接由 §7.1 的函数方程得证. 至于 (2), 将在 §10.3(c) 中予以说明.

表 10.3　$\zeta(1-r)$ 的表

$$\zeta(-1) = -\frac{1}{12} = -\frac{1}{2^2\cdot 3}$$
$$\zeta(-3) = \frac{1}{120} = \frac{1}{2^3\cdot 3\cdot 5}$$
$$\zeta(-5) = -\frac{1}{252} = -\frac{1}{2^2\cdot 3^2\cdot 7}$$
$$\zeta(-7) = \frac{1}{240} = \frac{1}{2^4\cdot 3\cdot 5}$$
$$\zeta(-9) = -\frac{1}{132} = -\frac{1}{2^2\cdot 3\cdot 11}$$
$$\zeta(-11) = \frac{691}{32760} = \frac{691}{2^3\cdot 3^2\cdot 5\cdot 7\cdot 13}$$
$$\zeta(-13) = -\frac{1}{12} = -\frac{1}{2^2\cdot 3}$$
$$\zeta(-15) = \frac{3617}{8160} = \frac{3617}{2^5\cdot 3\cdot 5\cdot 17}$$
$$\zeta(-17) = -\frac{43867}{14364} = -\frac{43867}{2^2\cdot 3^3\cdot 7\cdot 19}$$
$$\zeta(-19) = \frac{174611}{6600} = \frac{283\cdot 617}{2^3\cdot 3\cdot 5^2\cdot 11}$$
$$\zeta(-21) = -\frac{77683}{276} = -\frac{131\cdot 593}{2^2\cdot 3\cdot 23}$$
$$\vdots$$

这样一来, 我们很好地了解了 $\zeta(1-r)$ 的分母, 而与此相反, 分子的情况则显得神秘. 看到了突然出现的 691 还有 3617 之类如此大的素数. 在分子中出现的最小的素数是 37, 它出现在

$$\zeta(-31) = 37\cdot 683\cdot 305065927/2^6\cdot 3\cdot 5\cdot 17$$

中. 进一步计算知它也出现在

$$\zeta(-67) = 37\cdot 101\cdot 123143\cdot 1822329343\cdot 5525473366510930028227481/2^3\cdot 3\cdot 5$$

中. (也可看出, 当 r 变大时, $\zeta(1-r)$ 变得分子要比分母大很多.) 进一步计算的话, 还知道 $\zeta(-31-36m)$ (m 为正整数) 的分子必定出现 37. 于是我们可以推测下面的断言会成立.

(∗) 设将 $\zeta(1-r)$ 写成既约分数时的分子为 N_r, 如果素数 p 除尽 N_r, 则对于任意的正整数 $m>0$, p 也除尽 $N_{r+(p-1)m}$.

实际上成立比 (∗) 更强的以下结果.

命题 10.4 (Kummer)　设 p 为素数, r 为不是 $p-1$ 的倍数的正偶数. 此时, 对于任意的正整数 $m>0$ 成立

$$\zeta(1-r) \equiv \zeta(1-r-(p-1)m) \pmod p.$$

这里对于两个有理数 α, β, 说 $\alpha \equiv \beta \pmod p$ 是指, 当把 $\alpha - \beta$ 写成既约分数时分子被 p 除尽. □

例如, 因为

$$\frac{1}{2^3 \cdot 3 \cdot 5} + \frac{1}{2^2 \cdot 3 \cdot 11} = \frac{21}{2^3 \cdot 3 \cdot 5 \cdot 11} \equiv 0 \pmod 7$$

故确实有 $\zeta(-3) \equiv \zeta(-9) \pmod 7$. (后面将看到, r 为 $p-1$ 的倍数时则 p 不能除尽 N_r. 因此命题 10.4 确实包含了 $(*)$.) 这个命题曾在第三章作为命题 3.24 叙述过. 比这个命题更一般的是下面的命题.

命题 10.5 设 p 为素数, n, r_1, r_2 为正整数, 且 r_1 不为 $p-1$ 的倍数. 如果 r_1 与 r_2 之间有关系 $r_1 \equiv r_2 \pmod{(p-1)p^{n-1}}$, 则成立

$$(1-p^{r_1-1})\zeta(1-r_1) \equiv (1-p^{r_2-1})\zeta(1-r_2) \pmod{p^n}. \quad \square$$

以上的那个同余式称做 **Kummer 同余式**. 为什么会发生这样的事呢? 在 (b) 以下的各小节中我们将论及在这种现象背后所存在的某种函数.

$\zeta(1-r)$ 的分子 N_r 有什么意义, 它又与什么样的对象有关联? 这些问题将在 §10.3(c) 中叙述. 按照最近的数学进展, 对于 N_r 知道的相当多了, 尽管如此, 还不能说了解 N_r 到了像了解 D_r 的程度, 还是具有神秘感.

在此我们给出一个最单纯的未解决问题. 如在表 10.3 的那样, 对于满足 $r+1<p$ 的素数 p, 作为除尽 N_r 的 p 还成立 $\mathrm{ord}_p(N_r)=1$. 根据对 $p<12,000,000$ 的计算也可以确认这个事实 (总而言之, 没有这样的 p 使得 p^2 除尽 N_r). 然而, 在一般情形下它成立吗? 我们也还不知道有什么反例, 我们也不知道能提什么样的猜想.

(b) p 进 L 函数

粗略地讲, 命题 10.5 说的是, 如果 r_1 和 r_2 在 p 进拓扑下相近的话, 则

$$(1-p^{r_1-1})\zeta(1-r_1) \quad 与 \quad (1-p^{r_2-1})\zeta(1-r_2)$$

在 p 进拓扑下也很相近. 设 $\mathbb{Z}_p$ 为 p 进整数环 ($\mathbb{Z}$ 按照 p 进拓扑的完备化). 若取 $r>0$ 为不是 $p-1$ 的倍数的正整数, 则由命题 10.3 知 $\zeta(1-r)$ 的分母不能被 p 除尽, 从而可以将 $\zeta(1-r)$ 看作是 $\mathbb{Z}_p$ 的元. 因此可以作下面那样的考虑.

我们固定一个非 $p-1$ 倍数的正整数 r_0, 那么对于满足 $r \equiv r_0 \pmod{p-1}$ 的正整数 r, 是否存在使得 $f_{r_0}(1-r) = (1-p^{r-1})\zeta(1-r)$ 的连续函数 $f_{r_0}: \mathbb{Z}_p \to \mathbb{Z}_p$? ($\mathbb{Z}_p$ 是 p 进拓扑) 实际上, 这样的连续函数确实存在, 并具有显著的性质.

在这一小节中, 我们要讲述存在有作为对于一般 Dirichlet L 函数的 p 进版的 p 进 L 函数. 而关于它的显著的性质则放在 (c) 以下的小节中去叙述.

设 N 为正整数,

$$\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$$

为 Dirichlet 特征, $L(s,\chi)$ 为 Dirichlet L 函数 (参照 §3.1). 在这里所说的 Dirichlet 特征, 我们常常考虑的是本原特征. 特别地, N 为 χ 的导子. 下面我们来考察对于素数 p, $L(s,\chi)$ 值的 p 进现象. 这时我们将 $\mathbb{Q}$ 在 $\mathbb{C}$ 中的代数闭包 $\overline{\mathbb{Q}}$ 嵌入到 p 进域 $\mathbb{Q}_p$ ($\mathbb{Q}$ 在 p 进拓扑下的完备化) 的代数闭包 $\overline{\mathbb{Q}_p}$ 中. 在下面固定这样一个嵌入, 并考虑 χ 像下面的那样在 $\overline{\mathbb{Q}_p}^\times$ 中的取值:

$$\chi : (\mathbb{Z}/N)^\times \to \overline{\mathbb{Q}_p}^\times .$$

首先定义 **Teichmüller 特征**

$$\begin{aligned}\omega &: (\mathbb{Z}/p)^\times \to \mathbb{Z}_p^\times \quad (p\text{为奇素数})\\ \omega &: (\mathbb{Z}/4)^\times \to \mathbb{Z}_2^\times \quad (p=2).\end{aligned}$$

对于 $\mathbb{Z}_p$ 的乘法群 $\mathbb{Z}_p^\times$ 有下面的基本事实 (参照第二章命题 2.16).

$$\mathbb{Z}_p^\times = \begin{cases}(\mathbb{Z}/p)^\times \times (1+p\mathbb{Z}_p) & p\text{为奇素数}\\ (\mathbb{Z}/4)^\times \times (1+4\mathbb{Z}_2) & p=2.\end{cases}$$

这里的群结构对于奇素数 p 而言, $(\mathbb{Z}/p)^\times$ 为 $p-1$ 阶循环群, $1+p\mathbb{Z}_p$ 是按乘法构成的群, 它同构于按照加法构成的群 $\mathbb{Z}_p$. 这个同构映射是存在的, 譬如

$$\frac{1}{p}\log : 1+p\mathbb{Z}_p \to \mathbb{Z}_p \quad \left(\frac{1}{p}\log(1+px) = \frac{1}{p}\sum_{n=1}^{\infty}(-1)^{n-1}\frac{(px)^n}{n}\right),$$

(其逆映射为 $x \mapsto \exp(px) = \sum\limits_{n=0}^{\infty}\dfrac{(px)^n}{n!}$). 而对于 $p=2$, $(\mathbb{Z}/4)^\times$ 为 2 阶循环群, $1+4\mathbb{Z}_2$ 同样地同构于加法群 $\mathbb{Z}_2$ (使用 $\dfrac{1}{4}\log$ 即可). 按照这个分解, 元 $(a,1)\in(\mathbb{Z}/p)^\times\times(1+p\mathbb{Z}_p)$ ($p=2$ 时为 $(\mathbb{Z}/4)^\times\times(1+4\mathbb{Z}_2)$) 可以看成是 $\mathbb{Z}_p^\times$ 的 $p-1$ 次单位根 ($p=2$ 时为 2 次根). 因此, $\omega : (\mathbb{Z}/p)^\times \to \mathbb{Z}_p^\times$ ($p=2$ 时, $\omega : (\mathbb{Z}/4)^\times \to \mathbb{Z}_2^\times$) 被 $\omega(a)=(a,1)$ 所决定. 对于奇素数 p, $\omega(a)$ 是满足 $\omega(a) \mod p = a$ 的 $\mathbb{Z}_p^\times$ 中的唯一的一个 $p-1$ 次单位根. 对于 $p=2$ 有 $\omega(a)=\pm1$, 且满足 $\omega(a) \mod 4 = a$. 像通常的 Dirichlet 特征那样定义 ω 使 $\omega(p\mathbb{Z})=0$, 则变为考虑函数 $\omega:\mathbb{Z}\to\mathbb{Z}_p^\times$ 了.

问题 2　对于奇素数 p 与整数 a, 证明数列 $\{a^{p^n}\}_{n\geqslant 0}$ 在 $\mathbb{Z}_p$ 中收敛. 证明其等于 $\omega(a)$. 当 $p=2$ 时, 对于奇数 a, 证明有 $\omega(a)=(-1)^{\frac{a-1}{2}}$.

我们在 (b) 小节的目的是要叙述下面的定理. 该定理是说, 在 L 函数于负整数处取的各个值之间的 p 进关系背后, 所明显存在的 p 进连续函数, 如同原本的 L 函数为 $\mathbb{C}$ 上的全纯函数那样, 这个 p 进连续函数不仅仅是 p 进连续的, 而且是 "p 进全纯" 的函数. 称将所有整数映为 1 的特征为**平凡特征 (trivial character)**, 以 **1** 表示.

定理 10.6 (久保田, Leopoldt)

(1) 设 $\chi : (\mathbb{Z}/N)^\times \to \overline{\mathbb{Q}_p}^\times$ 为 Dirichlet 特征, 且 $\chi \neq \mathbf{1}$. 这时存在唯一的从 $\mathbb{Z}_p$ 到 $\overline{\mathbb{Q}_p}$ 的 p 进全纯函数 $s \mapsto L_p(s,\chi)$ ($s \in \mathbb{Z}_p$, $L_p(s,\chi) \in \overline{\mathbb{Q}_p}$), 使得对于任意的正整数 $r > 0$ 满足

$$L_p(1-r,\chi) = (1-\chi\omega^{-r}(p)p^{r-1})L(1-r,\chi\omega^{-r}).$$

其中, 在 $\overline{\mathbb{Q}_p}^\times$ 中取值的 Dirichlet 特征是根据我们所固定的嵌入 $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ 给出的通常意义下的 Dirichlet 特征, 并考虑成复的 Dirichlet L 函数. 所谓 p 进全纯函数是指, 对于任意的 $\alpha \in \mathbb{Z}_p$, 存在 $a_n \in \overline{\mathbb{Q}_p}$ 的 $\{a_n\}_{n\geqslant 0}$, 使得对于任意的 $s \in \mathbb{Z}_p$ 可以展开为幂级数

$$L_p(s,\chi) = \sum_{n=0}^{\infty} a_n(s-\alpha)^n \quad (\text{对于所有的 } s \in \mathbb{Z}_p)$$

的函数.

(2) 对于平凡特征 $\mathbf{1}$, p 进亚纯函数 $L_p(s,\mathbf{1})$ 有定义. $L_p(s,\mathbf{1})$ 在 $\mathbb{Z}_p \setminus \{1\}$ 上为 p 进全纯, 是取值于 $\overline{\mathbb{Q}_p}$ 的函数, 且 $s=1$ 是其留数为 $1-\frac{1}{p}$ 的一阶极点. 对于任意的正整数 $r>0$ 满足

$$L_p(1-r,\mathbf{1}) = (1-\omega^{-r}(p)p^{r-1})L(1-r,\omega^{-r}).$$

满足这个性质的函数也是唯一的. □

称 $L_p(s,\chi)$ 为**久保田–Leopoldt p 进 L 函数** (p-adic L function). 由于 $\{1-r \mid r \in \mathbb{Z}_{>0}\}$ 在 $\mathbb{Z}_p$ 中稠密, 故而定理 10.6 中仅在 $1-r$ 的值就决定了该函数. 现考虑 χ 为 Dirichlet 特征, r_0 为任意整数的 p 进 L 函数 $L_p(s,\chi\omega^{r_0})$. 根据定理 10.6, 对于满足 $r \equiv r_0 \pmod{p-1}$ 的任意正整数 r (但 $p=2$ 时为 $r \equiv r_0 \pmod 2$) 成立

$$L_p(1-r,\chi\omega^{r_0}) = (1-\chi(p)p^{r-1})L(1-r,\chi). \tag{10.2}$$

即便在这些值的范围内, 也可给予 $L_p(s,\chi\omega^{r_0})$ 以特征描述. 之所以这样说是因为在 $\{1-r \mid r \in \mathbb{Z}_{>0},\ r \equiv r_0 \pmod{p-1}\}$ 的 (p 进拓扑下的) 闭包上的值完全决定了幂级数展开式的系数.

又由上面的性质 (10.2) 可知, 我们在本小节 (b) 开始处曾推测存在的 f_{r_0} 恰好就是 $L_p(s,\omega^{r_0})$.

一般地, 对于 Dirichlet 特征 χ, 我们称 $\chi(-1)=1$ 的 χ 为偶特征, 而 $\chi(-1)=-1$ 的 χ 为奇特征. 对于奇特征 χ 与正偶数 r, 有 $L(1-r,\chi)=0$. 另外对于偶特征 χ 与正奇数 r, 除去 $\chi=\mathbf{1}, r=1$ 外, 也有 $L(1-r,\chi)=0$. 于是, 由定理 10.6 中 $L_p(s,\chi)$ 的性质, 如果考虑到 ω 为奇特征的话, 则当 χ 为奇特征时 $L_p(s,\chi)$ 恒等于零. 因此, 我们的兴趣便在偶特征 χ 的 p 进 L 函数 $L_p(s,\chi)$ 上了.

在定理 10.6 对 $L_p(s,\chi)$ 做特征描述时出现的 $1-\chi\omega^{-r}(p)p^{r-1}$ 是在 p 的 Euler 因子. 因为像 $1-\chi\omega^{-r}(p)p^{-s}$ 这样的函数离 p 进连续函数还很远, 所以除此以外

还必须有其他的东西. 对于任意的 Dirichlet 特征 χ, 定义 $\mathbb{C}$ 上的函数 $L_{\{p\}}(s,\chi)$ 为 $L_{\{p\}}(s,\chi)=(1-\chi(p)p^{-s})L(s,\chi)$, 并以

$$L_p(1-r,\chi)=L_{\{p\}}(1-r,\chi\omega^{-r})$$

给出刻画 p 进 L 函数特征的表达式.

我们在此不去直接证明定理 10.6. 在下面的 (c) 小节中将要叙述比 $L_p(s,\chi)$ 为 p 进全纯函数更强的性质, 并在后面的 (e) 给出证明.

另外关于 $L_p(s,\mathbf{1})$ 在 $s=1$ 具有一阶极点, 我们来给点评注. 因为我们是从 $\zeta(1-r)$ 的 p 进性质出发来作 p 进 L 函数的, 所以在正整数的值无论如何都应当是没有问题的. 虽然如此, 似乎是对应于 $\zeta(s)$ 在 $s=1$ 具有一阶极点那样, 我们惊讶地发现 $L_p(s,\mathbf{1})$ 在 $s=1$ 也有一阶极点. 其原因并不是这样的 p 进 L 函数可由复 L 函数在负整数的值偶然地、人为地做出来的, 而是有着某种更深层的原因. 再有, 对于全实数域而言, 称同样的命题 "全实数域 K 的 p 进 L 函数 $L_{p,K}(s,\mathbf{1})$ (本书将不对此定义) 在 $s=1$ 具有一阶极点" 为 Leopoldt 猜想, 这是一个尚未解决的难题.

(c) 岩泽函数

在前一小节叙述了 p 进 L 函数具有 "p 进全纯" 这样好的性质. 比起仅仅是连续来这是一个更强的性质, 实际上 p 进 L 函数是具有更加强大的收敛性的函数. 本小节的目的是要讲述具有这些突出性质的 p 进 L 函数, 即岩泽函数.

设 χ 为取值于 $\overline{\mathbb{Q}_p}$ 的 Dirichlet 特征, 并设 $O_\chi=\mathbb{Z}_p[\mathrm{Im}\chi]$ 为 $\mathbb{Z}_p$ 上由 χ 的像生成的完备离散赋值环. 由于此处的 $\mathrm{Im}\chi$ 是 $\overline{\mathbb{Q}_p}^\times$ 中的有限群, 故而我们注意到, 存在某个 $r>0$ 使得其可以写为 $\mathrm{Im}\chi=\mu_r$ (r 次单位根全体). 特别地, O_χ 的商域为 $\mathbb{Q}_p$ 的有限扩域.

如同在 (b) 小节所见, 当 p 为奇素数时 $\mathbb{Z}_p^\times$ 的子群 $1+p\mathbb{Z}_p$ 同构于加法群 $\mathbb{Z}_p$. 而当 $p=2$ 时 $\mathbb{Z}_2^\times$ 的子群 $1+4\mathbb{Z}_2$ 则同构于 $\mathbb{Z}_2$. 为了能将奇素数的情形与 $p=2$ 的情形统一表示, 我们都使用 $1+2p\mathbb{Z}_p$ 来表示. 设 u 为 $1+2p\mathbb{Z}_p$ 的拓扑生成元. 也就是说, 取 u 使得 $u-1$ 被 $2p$ 除尽而不被 $2p^2$ 除尽 (例如 p 为奇素数时取 $u=1+p$ 即可). 将 $1+2p\mathbb{Z}_p$ 的任意元写成 $u^\alpha, \alpha\in\mathbb{Z}_p$ 的形式. 设 $u=1+2pu'$ 从而 $u^\alpha=1+2pu'\alpha+(2pu')^2\cdot\dfrac{\alpha(\alpha-1)}{2}+\cdots$.

定理 10.7 (岩泽) *固定 $1+2p\mathbb{Z}_p$ 的一个 (拓扑) 生成元 u.*

(1) 设 $\mathrm{Frac}\,(O_\chi[[T]])$ 为形式幂级数环 $O_\chi[[T]]$ 的商域. 对于 Dirichlet 特征 χ, 存在 $\mathrm{Frac}\,(O_\chi[[T]])$ 的元 $G_\chi(T)\in\mathrm{Frac}\,(O_\chi[[T]])$ 满足

$$L_p(s,\chi)=G_\chi(u^s-1).$$

(2) 当 χ 的导子既非 1 又非 p^n $(n\geqslant 2)$ 时, $G_\chi(T)$ 自身便是 $O_\chi[[T]]$ 中的元. 更准确地说是 $\dfrac{1}{2}G_\chi(T)\in O_\chi[[T]]$. □

由此定理能够知道非常多的东西. 首先, 自然涌现的疑问是幂级数 (的商)$G_\chi(T)$ 具有何种意义? 实际上回答这个问题也可以说成是整个本章的目的. 其次, 我们能知道可由幂级数表示的 $L_p(s,\chi)$ 具有非常强的收敛性. 当记 $u=1+2pu'$, $u'\in\mathbb{Z}_p$ 时, 则 u^s 可以展开为幂级数

$$\begin{aligned}u^s &= (1+2pu')^s\\ &= 1+2pu's+\frac{(2p)^2}{2}u'^2s(s-1)+\cdots\\ &\qquad\cdots+\frac{(2p)^n}{n!}u'^ns(s-1)\cdots(s-n+1)+\cdots.\end{aligned}$$

观察上式就可知道 s^n 项的系数必定被 $(2p)^n/n!$ 除尽.

因此, 对于任意的幂级数 $F(T)\in O_\chi[[T]]$, 当记 $F(u^s-1)=\sum\limits_{n=0}^{\infty}a_ns^n$ 时, 对于所有的 $n\geqslant 1$, a_n 均被 $(2p)^n/n!$ 除尽. 在 $n\to\infty$ 时, $(2p)^n/n!$ 在 p 进拓扑下非常快地趋向于 0. 实际上, 设 ord_p 为 p 所决定的正规离散赋值 (即被 p 除尽的次数, 参看定义 1.15), 那么因为由下面的问题 3 知 $\mathrm{ord}_p(n!)<\dfrac{n}{p-1}$, 故得到以下的

$$\mathrm{ord}_p\left(\frac{(2p)^n}{n!}\right)=\begin{cases}n-\mathrm{ord}_p(n!)>(1-\dfrac{1}{p-1})n & p\neq 2\\ 2n-\mathrm{ord}_p(n!)>n & p=2.\end{cases}$$

问题 3 证明, 当 $n=a_0+a_1p+\cdots+a_rp^r$, $0\leqslant a_0,a_1,\cdots,a_r\leqslant p-1$ 时,

$$\mathrm{ord}_p(n!)=\sum_{i=0}^{r}a_i(p^i-1)/(p-1).$$

从上面的定理 10.7 可以得到以下的命题.

命题 10.8 设 χ 的导子既非 1 也非 $p^2,p^3,\cdots$ 的 Dirichlet 特征. 对 $\alpha\in\mathbb{Z}_p$, 设 p 进 L 函数 $L_p(s,\chi)$ 的 Taylor 展开为

$$L_p(s,\chi)=\sum_{n=0}^{\infty}a_n(s-\alpha)^n,$$

则对于 $n\geqslant 1$, 系数 $a_n\in O_\chi$ 被 $2\cdot\dfrac{(2p)^n}{n!}$ 除尽. 特别地成立

$$\begin{aligned}\mathrm{ord}_p(a_n) &>\left(1-\frac{1}{p-1}\right)n \quad (p\neq 2)\\ &> n+1 \qquad\qquad (p=2).\end{aligned}$$

这里的 $\mathrm{ord}_p: O_\chi\to\mathbb{Q}$ 是以 $\mathrm{ord}_p(p)=1$ 正规化的 O_χ 的离散赋值. □

这样, 将 u^s-1 代入该幂级数所得到的函数便称做**岩泽函数**(Iwasawa function).

由命题 10.8 知, 对于所有 $n \geqslant 1$, a_n 至少也是在 O_χ 的极大理想之中. 由于命题 10.5 可以直接从这个事实中推导出来, 我们现在便来叙述它.

命题 10.5 (Kummer 同余式) 的证明　设 r_0 为整数, 且 $r_0 \not\equiv 0 \pmod{p-1}$. 于是 p 必定为奇素数, 又 $\omega^{r_0} \neq \mathbf{1}$. 由于 ω^{r_0} 的导子为 p, 故而可以应用命题 10.8. 当展开幂级数

$$L_p(s, \omega^{r_0}) = \sum_{i=0}^{\infty} a_i (s - 1 + r_0)^i \quad (a_i \in \mathbb{Z}_p)$$

时, 由上述的命题 10.8 知, 对于所有的 $i \geqslant 1$, p 除尽 a_i. 因此对于满足 $r \equiv r_0 \pmod{(p-1)p^{n-1}}$ 的任意 r 成立

$$L_p(1 - r, \omega^{r_0}) = \sum_{i=0}^{\infty} a_i (r_0 - r)^i \equiv a_0 \pmod{p^n}.$$

如果再有 r 为正整数的话, 那么由 $L_p(1 - r, \omega^{r_0}) = (1 - p^{r-1})\zeta(1 - r)$, 我们便有

$$(1 - p^{r-1})\zeta(1 - r) \equiv a_0 \pmod{p^n},$$

故而对于这样的 r, $(1 - p^{r-1})\zeta(1 - r) \bmod p^n$ 固定不变. □

问题 4　取 p 为奇素数, r_1 为正偶数, 且 $r_1 \not\equiv 0 \pmod{p-1}$, 并设 $G_{\omega^{r_1}}(T) \in \mathbb{Z}_p[[T]]$ 为定理 10.7 所保证存在的那个幂级数. 在写成

$$G_{\omega^{r_1}}(T) = \sum_{i=0}^{\infty} A_i T^i \in \mathbb{Z}_p[[T]]$$

时, 我们假定 A_1 被 p 除尽. 证明, 对于任意的正整数 $r_2 > 0$ 和 $n > 0$, 如果有 $r_1 \equiv r_2 \pmod{(p-1)p^{n-1}}$, 则成立

$$(1 - p^{r_1-1})\zeta(1 - r_1) \equiv (1 - p^{r_2-1})\zeta(1 - r_2) \pmod{p^{n+1}}.$$

(成立比 Kummer 同余式 (命题 10.5) 中 p 的幂大 1 的同余式. 我们还不知道有 A_0 和 A_1 都被 p 除尽的这样的 p 的实际例子.)

定理 10.7 的证明将在 (e) 小节中给出. 下面我们要叙述对于幂级数 $G_\chi(T)$ 非常重要的定理.

定理 10.9 (Ferrero-Washington)　假设 χ 为偶特征 ($\chi(-1) = 1$), 其导子既非 1 也非 $p^2, p^3, \ldots$. 并设 π 为离散赋值环 O_χ 的极大理想的生成元, 而 $G_\chi(T)$ 为定理 10.7 中那样的幂级数, 则 $\frac{1}{2}G_\chi(T)$ 不被 π 除尽. 也就是说当写成

$$\frac{1}{2}G_\chi(T) = \sum_{i=0}^{\infty} A_i T^i \in O_\chi[[T]]$$

时, A_i 中至少有一个不被 π 除尽. □

这个 Ferrero–Washington 定理的意义及其重要性在 §10.2 以后将会变得清楚明白. 该定理的证明将在 (g) 小节给出.

(d) 群环与完备群环

为了研究 p 进 L 函数的更深入的性质, 有必要了解群环的知识. 因此, 我们在此要叙述有关的群环和完备群环.

设 R 为交换环, G 为有限群 (其运算以乘法记之), 这时我们定义 G 在 R 上的**群环** $R[G]$ 如下. $R[G]$ 的元是 G 的元以 R 为系数所形成的线性组合式

$$\sum_{\sigma\in G} a_\sigma\sigma \qquad (a_\sigma \in R).$$

在 $R[G]$ 中的和与积自然地予以定义, 即定义

$$\sum_{\sigma\in G} a_\sigma\sigma + \sum_{\sigma\in G} b_\sigma\sigma = \sum_{\sigma\in G}(a_\sigma + b_\sigma)\sigma$$

$$\left(\sum_{\sigma\in G} a_\sigma\sigma\right)\cdot\left(\sum_{\sigma\in G} b_\sigma\sigma\right) = \sum_{\substack{\sigma\in G\\ \tau\in G}} a_\sigma b_\tau \sigma\tau = \sum_{\sigma\in G} c_\sigma\sigma$$

(其中 $c_\sigma = \sum\limits_{\substack{\alpha,\beta\in G\\ \alpha\beta=\sigma}} a_\alpha b_\beta$). $R[G]$ 作为 R 模 (在日本叫做 R 加群—译注) 是秩为 $\#G$ 的自由 R 模.

下面定义完备群环. 设 G 为投射有限 (profinite) 群, 即 $G = \varprojlim G_i$ (G_i 为有限群). 譬如, $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i$ 以及无限 Galois 扩域的 Galois 群都为投射有限群. 这时, 定义 G 在 R 上的**完备群环** $R[[G]]$ 为

$$R[[G]] = \varprojlim R[G_i] \qquad (G = \varprojlim G_i).$$

在这里, 逆向系 (G_i) 的映射 $f_{ji} : G_j \to G_i$ 自然地给出映射 $R[G_j] \to R[G_i]$: $\sum\limits_{\sigma\in G_j} a_\sigma\sigma \mapsto \sum\limits_{\sigma\in G_j} a_\sigma f_{ji}(\sigma)$, 这个逆向极限 $\varprojlim R[G_i]$ 便是关于这个自然映射的. 当 G 为有限群时, $R[[G]]$ 与 $R[G]$ 相同.

我们将要在本章中多次应用下面的这个命题.

命题 10.10 设 R 为 p 进分离完备, 即满足 $R = \varprojlim R/p^nR$ 的环. (例如,, R 为完备离散赋值环, 其商域的特征为 0, 而剩余域的特征为 $p > 0$.) 考虑完备群环 $R[[\mathbb{Z}_p]]$, 其中 $\mathbb{Z}_p$ 被看做加法群. 对于 $\mathbb{Z}_p$ 的元 $\alpha \in \mathbb{Z}_p$, 以 $[\alpha] \in R[[\mathbb{Z}_p]]$ 表示对应的在完备群环中的元. 于是, 存在单变量形式幂级数 $R[[T]]$ 与 $R[[\mathbb{Z}_p]]$ 间的同构映射:

$$R[[T]] \xrightarrow{\sim} R[[\mathbb{Z}_p]]$$
$$f(T) \mapsto f([1]-1).$$

其中 $f([1]-1)$ 的准确意思如下. 对于 $a\in\mathbb{Z}$ 设 $[a \bmod p^i]$ 表示其在 $R[\mathbb{Z}/p^i]$ 中对应的元, 那么 $f([1 \bmod p^i]-1)$ 则可看作 $R[\mathbb{Z}/p^i]$ 的元, 从而构成了一个逆向系. 记其逆向极限为 $f([1]-1)$.

特别地, 对于任意的 $\alpha\in\mathbb{Z}_p$, 按照这个同构 $[\alpha]\in R[[\mathbb{Z}_p]]$ 对应于 $(1+T)^\alpha = 1+\alpha T+\dfrac{\alpha(\alpha-1)}{2}T^2+\cdots$.

[证明] 将 $R[\mathbb{Z}/p^i]$ 的元 $[1 \bmod p^i]$ 写为 $1+T$, 则给出了环同构

$$R[\mathbb{Z}/p^i]\xrightarrow{\sim} R[T]/((1+T)^{p^i}-1)$$
$$[1 \bmod p^i]\mapsto 1+T.$$

它的逆映射为 $f(T) \bmod (1+T)^{p^i}-1\mapsto f([1 \bmod p^i]-1)$. 因此由以下引理便得到了命题 10.10. □

引理 10.11 设 R 为命题 10.10 中的样子, 于是

$$\varprojlim R[T]/((1+T)^{p^i}-1)\simeq R[[T]].$$

[证明] 首先我们注意到, 由于 R 为 p 进完备 (即 $R=\varprojlim R/p^iR$), 故而

$$R[[T]]=\varprojlim R[T]/(T^i)=\varprojlim R[T]/(p^i,T^i)=\varprojlim R[T]/(p,T)^i$$
$$\varprojlim R[T]/((1+T)^{p^i}-1)=\varprojlim R[T]/(p^i,(1+T)^{p^i}-1).$$

因此, 如果能证明对于任意正整数 i 存在某个正整数 j 使得 $(p,T)^j\subset(p^i,(1+T)^{p^i}-1)$, 以及对于任意的正整数 i 存在某个正整数 j 使得 $(p^j,(1+T)^{p^j}-1)\subset(p,T)^i$ 就可以了. 于是我们只需证明

(1) 对于任意 i, 如果取 j 充分大, 则有 $T^j\in(p^i,(1+T)^{p^i}-1)$,

(2) 对于任意 i, 如果取 j 充分大, 则 $(1+T)^{p^j}-1\in(p,T)^i$.

对于 (1), 因为 $T^{p^i}\in(p,(1+T)^{p^i}-1)$, 故成立

$$(T^{p^i})^i=T^{p^i i}\in(p^i,(1+T)^{p^i}-1).$$

对于 (2), 我们有

$$(1+T)^{p^i}-1=\frac{(1+T)^{p^i}-1}{(1+T)^{p^{i-1}}-1}\cdot\cdots\cdot\frac{(1+T)^{p^2}-1}{(1+T)^p-1}\cdot((1+T)^p-1),$$

由于右端的 i 个元全都属于 (p,T), 故知 $(1+T)^{p^i}-1\in(p,T)^i$. 这样, 引理 10.11 得证. □

后面还要使用关于群环的如下事实.

命题 10.12 设 R 为交换环, G 为 n 阶有限 Abel 群. 假设 $\dfrac{1}{n} \in R$, 并且 R 包含了 n 次本原单位根. 以 $\widehat{G} = \mathrm{Hom}\,(G, R^\times)$ 表示从 G 到 $R^\times$ 的全体同态. 于是

(1) 对于 $\chi \in \widehat{G}$ 令

$$e_\chi = \frac{1}{n}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1} \in R[G],$$

则 e_χ 满足 $e_\chi^2 = e_\chi$, $e_\chi\sigma = \chi(\sigma)e_\chi$, $\sum\limits_{\chi\in\widehat{G}} e_\chi = 1$, $e_\chi\cdot e_{\chi'} = 0\,(\chi\neq\chi')$.

(2) 设 M 为 $R[G]$ 模, 则 M 可分解为

$$M = \bigoplus_{\chi\in\widehat{G}} e_\chi M.$$

[证明] (1) 只需经过通常的计算即可. (2) 则由 (1) 得到. 实际上由 $1 = \sum e_\chi$, 对任意的 $x \in M$, 可写为 $x = \sum e_\chi \cdot x$. 若有 $\sum e_\chi a_\chi = 0$ $(a_\chi \in M)$, 那么由 $e_\chi^2 = e_\chi$, $e_\chi\cdot e_{\chi'} = 0\,(\chi\neq\chi')$ 知, 当乘以对任意 χ 的 e_χ 时得到 $e_\chi a_\chi = 0$. 因此这是个直和分解, (2) 得证. ∎

(e) Galois 群与 p 进 L 函数

我们由 ζ 函数以及 L 函数的特殊值能够定义称为 p 进 L 函数的 p 进连续函数, 它不仅是 p 进连续的而且是 p 进全纯的, 还看到了它不仅是 p 进全纯的而且还是岩泽函数. 也就是说, p 进 L 函数的本质是某个形式幂级数 $G_\chi(T)$. 在这个 (e) 小节中将讲述 p 进 L 函数实际附着在 Galois 群的群环之上这个事实. 这是个只比岩泽函数强一点的事实.

考虑连续同态 $\chi: G \to L^\times$ (L 为 $\mathbb{Q}_p$ 的有限扩域), 其中 G 作为交换的投射有限群但其像不一定有限. 这个映射可像下面那样延拓为环的连续同态 $\chi: \mathbb{Z}_p[[G]] \to L$. 设 $G = \varprojlim G/H$, (H 遍历 G 的开子群), 以 $\mu \in \mathbb{Z}_p[[G]]$ 表示 $\mu = (\mu_H)$, $\mu_H = \sum a_{H,\sigma}\sigma \in \mathbb{Z}_p[G/H]$. 又设 I_H 为 $\{(\chi(h)-1)\chi(\sigma) \mid h \in H, \sigma \in G\}$ 生成的 $\mathbb{Z}_p$ 模, 那么在 $\bmod I_H$ 的意义下考虑 $\chi(\mu_H) = \sum a_{H,\sigma}\chi(\sigma)$. 当 H 接近 $\{1\}$ 时, I_H 则靠近 $\{0\}$, 故而当我们定义 $\chi(\mu_H)$ 的极限为 $\chi(\mu)$ 时便得到了上述那样的同态. 对于 $\chi(\mu)$ 我们可以将 χ 考虑为对由 μ 构成的测度的积分 (即 $\chi(\mu)$ 可写为 $\int \chi d\mu$), 但我们对此不再加阐述.

现在要考虑的是分圆域的 Galois 群. 对于正整数 n 以 μ_n 表示全体 n 次单位根, 而 $\mathbb{Q}(\mu_n)$ 表示在 $\mathbb{Q}$ 中添加全体 n 次单位根得到的域. 像在 §5.2 中所看到的那样, 我们有 $\mathrm{Gal}\,(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n)^\times$. 那么, 我们取 N_0 为与 p 互素的整数, 考虑 $\mathbb{Q}(\mu_{N_0p^\infty}) = \bigcup\limits_{n\geqslant 1}\mathbb{Q}(\mu_{N_0p^n})$, 于是有

$$\begin{aligned}\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) &= \varprojlim \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^n})/\mathbb{Q}) \simeq \varprojlim(\mathbb{Z}/N_0p^n)^\times \\ &\simeq \varprojlim(\mathbb{Z}/N_0)^\times \times (\mathbb{Z}/p^n)^\times = (\mathbb{Z}/N_0)^\times \times \mathbb{Z}_p^\times.\end{aligned}$$

由于像在 (b) 小节中那样我们有 $\mathbb{Z}_p^\times \simeq (\mathbb{Z}_p/2p)^\times \times \mathbb{Z}_p$, 那么, 使用这个同构便有:

$$
\begin{aligned}
(10.3) \qquad & \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) = \Delta \times \Gamma \\
& \Delta \simeq (\mathbb{Z}/N_0p)^\times \qquad p\text{为奇素数} \\
& \qquad (\mathbb{Z}/4N_0)^\times \qquad p = 2 \\
& \Gamma \simeq \mathbb{Z}_p.
\end{aligned}
$$

$\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$ 作用于全体 p^n 次单位根 μ_{p^n} 上, 从而也作用于 $\varprojlim \mu_{p^n}$ 上. 因为 $\varprojlim \mu_{p^n}$ 为秩为 1 的自由 $\mathbb{Z}_p$ 模, 故而这个作用可以用 $\mathbb{Z}_p^\times$ 的元表示. 确切地写出来就是, 对于 $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$ 存在唯一的 $\mathbb{Z}_p^\times$ 的元 α, 使得对于任意的 $n > 0$ 以及 $\zeta \in \mu_{p^n}$ 成立 $\sigma(\zeta) = \zeta^\alpha$. 记此 α 为 $\kappa(\sigma)$. 于是得到了同态映射

$$\kappa : \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times.$$

称这个映射为**分圆特征**. 在考虑上面的 Galois 群的分解 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \simeq (\mathbb{Z}/N_0)^\times \times \mathbb{Z}_p^\times$ 时, κ 正是其第二个分量的投影. 也可将 κ 考虑为

$$\kappa : \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \to \overline{\mathbb{Q}_p}^\times.$$

我们应注意, 相对于 Dirichlet 特征的像为有限群而言, κ 的像是无限群.

对于奇素数 p, 我们将

$$\mathrm{Gal}(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \xrightarrow{\kappa} \mathbb{Z}_p^\times \xrightarrow{\bmod p} (\mathbb{Z}/p)^\times$$

与在 (b) 中所叙述过的 Teichmüller 特征 $\omega : (\mathbb{Z}/p)^\times \to \mathbb{Z}_p^\times$ 复合, 则得到了同态 $\omega : \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times$. 在此我们仍然用了 ω 来表示它, 并仍然称它为 **Teichmüller 特征**. 对于 $p = 2$ 也同样, 简单地以 ω 表示 $\omega \circ \bmod 4 \circ \kappa$. 以 $\langle\kappa\rangle = \dfrac{\kappa}{\omega}$ 定义特征

$$\langle\kappa\rangle : \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times,$$

则可考虑对应于 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$ 的分解 (10.3) 的 κ 的分解 $\kappa = \omega\langle\kappa\rangle$. 在这里, 我们认为 ω 是 Δ 的特征, 而 $\langle\kappa\rangle$ 为 Γ 的特征.

我们再定义完备群环 Λ_{N_0} 为

$$\Lambda_{N_0} = \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})]].$$

记 Λ_{N_0} 的全商环为 $Q(\Lambda_{N_0})$. 就是说, $Q(\Lambda_{N_0})$ 为所有 $\dfrac{\alpha}{\beta}$ $(\alpha, \beta \in \Lambda_{N_0},\ \beta$ 为非零因子) 所构成的环. 现在我们定义

$$\widetilde{\Lambda_{N_0}} = \{\theta \in Q(\Lambda_{N_0}) \mid \text{对所有 } \sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \text{ 有 } (1-\sigma)\theta \in \Lambda_{N_0}\}.$$

$\Lambda_{N_0}^{\sim}$ 是 $Q(\Lambda_{N_0})$ 中的 Λ_{N_0} 模并包含了 Λ_{N_0}. 将 Λ_{N_0} 考虑为 $\mathrm{Gal}(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$ 的所有 $\mathbb{Z}_p$ 测度所构成的群. 那么则称 $\Lambda_{N_0}^{\sim}$ 为所有伪测度 (pseudo-measure) 构成的群. 我们在这里不打算深入到测度论的解释中去.

我们现在来给出 $\Lambda_{N_0}^{\sim}$ 的具体表示. 取 Γ 作为 $\mathbb{Z}_p$ 模的一个 (拓扑) 生成元 γ, 在分解 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) = \Delta\times\Gamma$ 中记 $(1,\gamma)$ 对应的元为 $\gamma_{N_0}\in\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$. 另外, 令 $N_\Delta=\sum\limits_{\sigma\in\Delta}(\sigma,1)\in\Lambda_{N_0}$. 于是, $\Lambda_{N_0}^{\sim}$ 可表示如下.

命题 10.13 设 γ_{N_0}, N_Δ 如上所示, 则

$$\Lambda_{N_0}^{\sim}=\frac{N_\Delta}{\gamma_{N_0}-1}\mathbb{Z}_p+\Lambda_{N_0}.$$

[证明] 首先证明右端在 $\Lambda_{N_0}^{\sim}$ 之中. 因为对于 $\sigma\in\Delta$ 有 $(1-(\sigma,1))N_\Delta=0$, 故有 $(1-(\sigma,1))$(右端) $\subset\Lambda_{N_0}$. 设 $\tau\in\Gamma$, 由于 γ 为 Γ 的生成元, 故可写成 $\tau=\gamma^\alpha$, $\alpha\in\mathbb{Z}_p$. 因此 $1-\tau$ 被 $\gamma-1$ 除尽. 所以我们有 $(1-(1,\tau))$(右端) $\subset\Lambda_{N_0}$. 一般地, 对于 $\sigma\in\Delta$, $\tau\in\Gamma$, 因为有 $1-(\sigma,\tau)=(1-(\sigma,1))(1,\tau)+1-(1,\tau)$, 故根据上面的结果有 $(1-(\sigma,\tau))$(右端)$\subset\Lambda_{N_0}$ 从而(右端) $\subset\Lambda_{N_0}^{\sim}$.

反之, 设 $x\in\Lambda_{N_0}^{\sim}$, 由 $(1-\gamma_{N_0})x\in\Lambda_{N_0}$, 并考虑 $\Lambda_{N_0}=\mathbb{Z}_p[\Delta]+(\gamma_{N_0}-1)\Lambda_{N_0}$, 则可写成

$$x=\frac{\alpha}{\gamma_{N_0}-1}+\beta,\quad \alpha=\sum_{\sigma\in\Delta}a_\sigma(\sigma,1),\ a_\sigma\in\mathbb{Z}_p,\ \beta\in\Lambda_{N_0}.$$

其次因为对于 $\sigma\in\Delta$ 有 $(1-(\sigma,1))x\in\Lambda_{N_0}$, 故 $(1-(\sigma,1))\alpha=0$, 最后得知 $(1-\sigma)\sum\limits_{\sigma\in\Delta}a_\sigma\sigma=0$. 由于这是对所有的 $\sigma\in\Delta$ 都成立, 故所有的 a_σ 都相等, 记其为 $\alpha=cN_\Delta$, $c\in\mathbb{Z}_p$. 这就是说 $\Lambda_{N_0}^{\sim}\subset$(右端). ∎

设 $\chi:\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})\to\overline{\mathbb{Q}_p}^\times$ 为像不一定有限的连续同态. 如在本小节一开始看到的那样, 由于线性性与连续性 (按照 $(\sum a_\sigma\sigma)\mapsto\lim\sum a_\sigma\chi(\sigma)$), χ 可延拓为环同态

$$\chi:\Lambda_{N_0}=\mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})]]\to\overline{\mathbb{Q}_p}.$$

在下面我们以同一个记号 χ 记这个环同态与群同态. 设 $\chi\neq\mathbf{1}$. 此时, 取 $\sigma\in\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$ 使得 $\chi(\sigma)\neq1$, 那么对于 $\theta\in\Lambda_{N_0}^{\sim}$, 我们定义 $\chi(\theta)=\chi((1-\sigma)\theta/(1-\chi(\sigma))$. 根据命题 10.13, 可写成 $\theta=\dfrac{N_\Delta}{\gamma_{N_0}-1}a+\theta'$, $a\in\mathbb{Z}_p$, $\theta'\in\Lambda_{N_0}$, 于是当 $\chi|_\Delta\neq\mathbf{1}$ 时使得 $\chi(\theta)=\chi(\theta')$, 而当 $\chi|_\Delta=\mathbf{1}$ 时使得 $\chi(\theta)=\dfrac{\#\Delta\cdot a}{\chi(\gamma_{N_0})-1}+\chi(\theta')$. 特别地, $\chi(\theta)$ 的定义不依赖于 σ 的选取. 这样一来, 对于 $\chi\neq\mathbf{1}$ 定义了

$$\chi:\Lambda_{N_0}^{\sim}=\mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})]]^{\sim}\to\overline{\mathbb{Q}_p}.$$

下面的定理是 §10.1 的主定理. 这个定理叙述了 p 进 ζ, z_{N_0} 位于群环 $\Lambda_{N_0}^{\sim}$ 之中的事实.

定理 10.14 对于与 p 互素的正整数 N_0, 存在唯一的满足下面性质 (*) 的元

$$z_{N_0} \in \Lambda_{N_0}^{\sim} = \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})]]^{\sim}.$$

设 χ 是取值于 $\overline{\mathbb{Q}_p}^\times$, 且其导子 N 除尽 N_0p^∞ 的任意 Dirichlet 特征. 这里所说的 "N 除尽 N_0p^∞" 是指, 存在某个整数 $a \geqslant 0$ 使得 N 除尽 N_0p^a (注意此时 χ 的像为有限). 设 $r>0$ 为任意正整数, κ 为分圆特征. 考虑将 $\chi\kappa^r\colon \mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) \to \overline{\mathbb{Q}_p}^\times$ 按照上面所说的那样延拓到群环的映射

$$\chi\kappa^r : \Lambda_{N_0}^{\sim} \to \overline{\mathbb{Q}_p}.$$

这时, 对于任意这样的 χ 和任意的 $r>0$, 在 $\chi\kappa^r$ 下 z_{N_0} 被写为

$$(*) \qquad \chi\kappa^r(z_{N_0}) = \left[\prod_{l|N_0p}(1-\chi(l)l^{r-1})\right] L(1-r,\chi).$$

右端的积遍历除尽 N_0p 的素数 l. 另外按照固定的 $\overline{\mathbb{Q}}$ 在 $\overline{\mathbb{Q}_p}$ 中的嵌入, 将 χ 看成是在 $\mathbb{C}^\times$ 中取值的 Dirichlet 特征, 也将 $L(s,\chi)$ 看成是复 L 函数. □

这个定理包含了比 p 进 L 函数只是岩泽函数要更深刻的信息.

我们将在后面的 (f) 小节中证明此定理. 在此我们在先承认这个定理的前提下来证明定理 10.6 和定理 10.7.

[定理 10.6 和定理 10.7 的证明] 设 χ 是导子为 N 的 Dirichlet 特征, 并记 $N=N_0p^a$, 其中 N_0 与 p 互素. 相伴于分解 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) = \Delta\times\Gamma$ 我们有 χ 的分解 $\chi=\chi_1\chi_2$ (χ_1 为 Δ 的特征, 而 χ_2 为 Γ 的特征). 当 p 为奇素数时 χ_1 的导子不被 p^2 除尽. χ_2 的导子或为 1 或为 $p^a (a\geqslant 2)$. 当 $p=2$ 时 χ_1 的导子不被 8 除尽, χ_2 的导子或为 1 或为 p^a $(a\geqslant 3)$. 一般地, 称 Δ 的特征为**第一类特征** (character of the first kind), 而称 Γ 的特征为**第二类特征** (character of the second kind).

从完备群环 $\Lambda_{N_0} = \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}]]$ 到完备群环 $O_{\chi_1}[[\Gamma]]$ $(O_{\chi_1} = \mathbb{Z}_p[\mathrm{Im}\chi_1])$ 的映射 ϕ_{χ_1} 定义为

$$\begin{aligned}\phi_{\chi_1} :&\Lambda_{N_0} \to O_{\chi_1}[[\Gamma]]\\ &\left(\sum a_{\sigma\tau}(\sigma,\tau)\right) \mapsto \left(\sum a_{\sigma\tau}\chi_1(\sigma)\tau\right).\end{aligned}$$

这里 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$ 的元按照分解 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q}) = \Delta\times\Gamma$ 可表示为 (σ,τ) $(\sigma\in\Delta, \tau\in\Gamma)$. 回想我们在定理 10.7 中曾固定过一个 $1+2p\mathbb{Z}_p$ 的乘法的拓扑生成元 u. 取 Γ 的生成元 γ 为满足 $\kappa(\gamma)=u$ 的元. 利用 γ 将 Γ 视为与 $\mathbb{Z}_p$ 等同. 于是根据命题 10.10 知 $O_{\chi_1}[[\Gamma]]$ 与单变量的形式幂级数环 $O_{\chi_1}[[T]]$ 同构. 具体地说, 对应的同构可以为

$$\begin{aligned}O_{\chi_1}[[\Gamma]] &\simeq O_{\chi_1}[[T]]\\ \gamma^\alpha &\leftrightarrow (1+T)^\alpha \quad (\alpha\in\mathbb{Z}_p).\end{aligned}$$

当然, 这个同构依赖于 u 的选取. 这样便得到了环同态

$$\phi_{\chi_1,u}: \Lambda_{N_0} \to O_{\chi_1}[[\Gamma]] \xrightarrow{\sim} O_{\chi_1}[[T]].$$

定义 $O_{\chi_1}[[T]]^{\sim} = \frac{1}{T}O_{\chi_1}[[T]]$, 则按照命题 10.13, 上面的 $\phi_{\chi_1,u}$ 可自然地延拓为

$$\phi_{\chi_1,u}: \Lambda_{N_0}^{\sim} \to O_{\chi_1}[[T]]^{\sim}.$$

在此, 我们注意到, 如果 $\chi_1 \neq \mathbf{1}$ 便有 $\phi_{\chi_1}(N_\Delta) = 0$, 故而由命题 10.13 知 $\phi_{\chi_1,u}$ 的像落入了 $O_{\chi_1}[[T]]$ 中. 也就是说, 当 $\chi_1 \neq \mathbf{1}$ 时, 定义了同态

$$\phi_{\chi_1,u}: \Lambda_{N_0}^{\sim} \to O_{\chi_1}[[T]].$$

现在取 $z_{N_0} \in \Lambda_{N_0}^{\sim}$ 为定理 10.14 所确保存在的元, 我们定义

$$g_{\chi_1}(T) := \phi_{\chi_1,u}(z_{N_0}) \in O_{\chi_1}[[T]]^{\sim}.$$

如上所说, 如果 $\chi_1 \neq \mathbf{1}$ 则有 $g_{\chi_1}(T) \in O_{\chi_1}[[T]]$. 现令

$$G_\chi(T) := g_{\chi_1}(\chi_2(\gamma)\kappa(\gamma)(1+T)^{-1}-1) \in \mathrm{Frac}\,(O_\chi[[T]]).$$

其中 $O_\chi = \mathbb{Z}_p[\mathrm{Im}\chi]$, $\mathrm{Frac}\,(O_\chi[[T]])$ 为 $O_\chi[[T]]$ 的商域. 按照定义, 对于正整数 $r > 0$, 可进行下面的计算:

$$\begin{aligned}
G_\chi(\kappa(\gamma)^{1-r}-1) &= g_{\chi_1}(\chi_2(\gamma)\kappa(\gamma)\kappa(\gamma)^{r-1}-1) \\
&= g_{\chi_1}(\chi_2(\gamma)\kappa(\gamma)^{r}-1) \\
&= \chi_1\chi_2\langle\kappa\rangle^r(z_{N_0}) \\
&= \chi\omega^{-r}\kappa^r(z_{N_0}) \\
&= (1-\chi\omega^{-r}(p)p^{r-1})L(1-r,\chi\omega^{-r}).
\end{aligned}$$

其中 $\langle\kappa\rangle = \frac{\kappa}{\omega}$, 在最后的那个等号处我们使用了 χ 的导子为 $N = N_0p^a$ 的事实以及定理 10.14. 因此, 如果定义

$$L_p(s,\chi) = G_\chi(\kappa(\gamma)^s - 1),$$

则它就成为在定理 10.6 所叙述的 p 进 L 函数.

由 $z_{N_0} \in \Lambda_{N_0}^{\sim}$ 及命题 10.13, 我们可记

$$g_{\chi_1}(T) = \frac{\chi_1(N_\Delta)c}{T} + g',\ c \in \mathbb{Z}_p,\ g' \in O_{\chi_1}[[T]].$$

于是我们可写出

$$G_\chi(T) = \frac{\chi_1(N_\Delta)c}{\chi_2(\gamma)\kappa(\gamma)(1+T)^{-1}-1} + G',\ c \in \mathbb{Z}_p,\ G' \in O_{\chi_1}[[T]],$$

从而可写

$$L_p(s,\chi)=\frac{\chi_1(N_\Delta)c}{\chi_2(\gamma)\kappa(\gamma)^{1-s}-1}+f,\quad c\in\mathbb{Z}_p,\ f\text{为}p\text{进全纯函数}.$$

注意, $\chi_2(\gamma)$ 为单位根, 如果 $\chi_2\neq\mathbf{1}$ 则 $\chi_2(\gamma)\neq 1$. 于是, 除去 $\chi=\mathbf{1}$, $s=1$ 外, 知道 $L_p(s,\chi)$ 在任意点都为 p 进全纯. 我们将在下面的 (f) 小节证明, 当 $\chi=\mathbf{1}$, $s=1$ 时, $L_p(s,\mathbf{1})$ 具有留数为 $1-\dfrac{1}{p}$ 的一阶极点. 除了这一点外, 定理 10.6 已得证.

下面证明定理 10.7. 如果想到我们取了 $\kappa(\gamma)=u$, 那么 (1) 已在上面证过了. 现在证明 (2). 设 χ 满足定理 10.7 (2) 的条件, 于是有 $\chi_1\neq\mathbf{1}$. 因此按照上面所说的那样我们有 $g_{\chi_1}(T)\in O_{\chi_1}[[T]]$, 从而 $G_\chi(T)\in O_\chi[[T]]$. 如果 p 为奇素数, 则因 $\dfrac{1}{2}\in O_\chi$, 立即得到 $\dfrac{1}{2}G_\chi(T)\in O_\chi[[T]]$. 下面设 $p=2$.

记在自然同构 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})\simeq(\mathbb{Z}/N_0)^\times\times\mathbb{Z}_p^\times$ 下, 对应于 $(-1,-1)$ 的元为 $\sigma_{-1}\in\mathrm{Gal}\,(\mathbb{Q}(\mu_{N_0p^\infty})/\mathbb{Q})$. 由 $\Lambda_{N_0}^\sim$ 的定义有 $(1-\sigma_{-1})z_{N_0}\in\Lambda_{N_0}$, 进而成立下面的断言.

断言 $(1-\sigma_{-1})z_{N_0}=0$.

[断言的证明] 设 ψ 为 $\Delta\simeq(\mathbb{Z}/4N_0)^\times$ 的特征, 如同上面那样, 考虑映射 $\phi_{\psi,u}:\Lambda_{N_0}^\sim\to O_\psi[[T]]^\sim$. 于是, 因为对于任意的奇特征 ψ, 像已经说过的那样有 $L_p(s,\psi)=0$, 故成立 $\phi_{\psi,u}(z_{N_0})=0$. 因此 $\phi_{\psi,u}((1-\sigma_{-1})z_{N_0})=0$. 对于 Δ 的偶特征 ψ, 由于 $\phi_{\psi,u}(1-\sigma_{-1})=1-\psi(-1)=0$ 这个等式总成立, 故而最后得知, 对于所有的 ψ 有 $\phi_{\psi,u}((1-\sigma_{-1})z_{N_0})=0$. 由此便推导出了 $(1-\sigma_{-1})z_{N_0}=0$. (要看出这点, 譬如设 Δ 的阶为 m; 由于只要能证明在 $\Lambda_{N_0}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p(\mu_m)=(\mathbb{Z}_p[[\Gamma]]\otimes\mathbb{Q}_p(\mu_m))[\Delta]$ 中 $(1-\sigma_{-1})z_{N_0}=0$ 就可以了, 故只要由命题 10.12 能证明 $e_\psi((1-\sigma_{-1})z_{N_0})=0$ 即可. 我们有 $e_\psi((1-\sigma_{-1})z_{N_0})=\phi_\psi((1-\sigma_{-1})z_{N_0})e_\psi$, 从而断言成立.) ∎

将 z_{N_0} 写成

$$z_{N_0}=\frac{N_\Delta}{\gamma_{N_0}-1}\cdot c+z'_{N_0},\quad c\in\mathbb{Z}_p,\ z'_{N_0}\in\Lambda_{N_0}.$$

由上面的断言有 $(1-\sigma_{-1})z'_{N_0}=0$. 回忆 $\Lambda_{N_0}=\mathbb{Z}_p[[\Gamma]][\Delta]$, 并记 $z'_{N_0}=\sum\limits_{\sigma\in\Delta}a_\sigma\sigma$, $a_\sigma\in\mathbb{Z}_p[[\Gamma]]$, 由此知成立 $a_\sigma=a_{\sigma\sigma_{-1}}$. 因此对第一类偶特征 $\chi_1\neq\mathbf{1}$ 有 $\phi_{\chi_1,u}(z_{N_0})\in 2O_{\chi_1}[[T]]$. 这便对于满足条件的偶特征 χ 推出了 $G_\chi(T)\in 2O_\chi[[T]]$. 另外对于奇特征 χ, 由于已经说过有 $G_\chi(T)=0$, 从而定理 10.7 得证. ∎

(f) 定理 10.14 的证明—Euler 方法的 p 进类比

在本 (f) 小节中将进行定理 10.14 的证明. 已知对定理 10.14 还有其他的不同证明. 譬如, 使用 Stickelberger 元的方法 (关于它, 我们将在 §10.3(d) 中谈及), 使用分圆单位的方法, 以及使用自守形式的方法. 这些方法由于直接与各种重要的数论对

象相联系故而很重要, 但在这里所考虑的不是上面的这些方法, 而是以类似于求 $\mathbb{C}$ 上 ζ 函数在负整数上值的方法来进行证明的. 我们避免那种使记号等徒然复杂化的一般情形, 而在此证明 $N_0=1$ 的情形. 于是, 我们想要证明的是存在具有定理中性质的元

$$z_1 \in \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]^\sim.$$

(如果其存在则由迄今的讨论知其唯一, 故这里只要证明存在性就可以了.) z_1 是作为对应于 Riemann ζ 的所谓 "p 进 Riemann ζ" 而存在的. 考虑 Riemann ζ 函数在整数的值, 于是对应于考虑在 z_1 的 $\kappa^n(z_1)$ $(n\in\mathbb{Z})$.

首先我们叙述 Euler 的对 Riemann ζ, 即 $\zeta(s)=\sum\limits_{n=1}^{\infty}\dfrac{1}{n^s}$ 在负整数上的求值办法. 设 $r>0$ 为正整数, 定义 t 的有理函数 $g_r(t)$ 为

$$g_r(t)=\left(t\frac{d}{dt}\right)^{r-1}\left(\frac{t}{1-t}\right).$$

由于当 $|t|<1$ 时有 $\dfrac{t}{1-t}=\sum\limits_{n=1}^{\infty}t^n$, 故在 $|t|<1$ 时有 $g_r(t)=\sum\limits_{n=1}^{\infty}n^{r-1}t^n$. 在此, 在我们的头脑里会浮现出能不能把 $\zeta(1-r)$ 计算成

$$g_r(1)=\sum_{n=1}^{\infty}n^{r-1}=\zeta(1-r)$$

呢? 这样的荒谬想法, 但由于 $g_r(t)$ 在 $t=1$ 具有极点, 因而这是不可能的. 于是 Euler 做了如下的考虑. 设 $c\geqslant 2$ 为不小于 2 的整数. 令

$$g_{1,c}(t)=g_1(t)-cg_1(t^c).$$

这样, $g_1(t)$ 与 $cg_1(t^c)$ 在 $t=1$ 的极点相互消去, 从而 $g_{1,c}(t)$ 在 $t=1$ 全纯. 现在令

$$g_{r,c}(t)=\left(t\frac{d}{dt}\right)^{r-1}g_{1,c}(t).$$

我们也将它写成 $g_{r,c}(t)=g_r(t)-c^rg_r(t^c)$. 因为 $g_{r,c}(t)$ 在 $t=1$ 全纯, 故 $g_{r,c}(1)$ 有意义. 于是, Euler 将 $g_{r,c}(1)$ 当作

$$\begin{aligned}g_{r,c}(1)&=\text{“}g_r(1)-c^rg_r(1)\text{”}\\&=(1-c^r)\zeta(1-r)\end{aligned}$$

来计算 $\zeta(1-r)$ 的值. 在这里的第一行的等式是一种没有明确意义的推测, 至于第二行的等式, 如果能用解析延拓概念的话则是可以严格证明的等式. 我们在此对这个方法进行简单的叙述. 设 D 为由 $D(\sum\limits_{n=1}^{\infty}a_nt^n,s)=\sum\limits_{n=1}^{\infty}a_nn^{-s}$ 定义的变换, 那么, 因为 $D(g_{1,c}(t),s)$ 具有积分表达式, 故可解析延拓为整个 $\mathbb{C}$ 上的全纯函数, 从而能证明

$D(g_{1,c}(t), 1-r) = g_{r,c}(1)$. 另一方面, 因为 $D(g_{1,c}(t), s) = (1-c^{1-s})\zeta(s)$, 从而得到了上面的等式. 我们因此处在了 p 进世界之中, 并成功证明了上面的公式, 但我们还是想看到 Galois 群而不是解析延拓所起到的重要作用.

以下设 p 为素数, 并做 p 进考虑. 设取 $c \geqslant 2$ 为与 p 互素的整数. $g_{1,c}(t)$ 可写为

$$g_{1,c}(t) = \frac{(c-1)t^{c-1} + (c-2)t^{c-2} + \cdots + t}{t^{c-1} + t^{c-2} + \cdots + 1}.$$

将 $t^{c-1} + t^{c-2} + \cdots + 1$ 看作为 $\mathbb{Z}_p[[t-1]]$ 的元时, 由于 $t^{c-1} + t^{c-2} + \cdots + 1 \equiv c \pmod{(t-1)}$ 以及 $c \not\equiv 0 \pmod{p}$, 故有 $t^{c-1} + t^{c-2} + \cdots + 1 \notin (p, t-1)$. 因为它不在局部环 $\mathbb{Z}_p[[t-1]]$ 的极大理想之中, 故 $t^{c-1} + t^{c-2} + \cdots + 1$ 为可逆元, 从而 $g_{1,c}(t)$ 为 $\mathbb{Z}_p[[t-1]]$ 中的元. 因此, 对于任意的 $r > 0$, $g_{r,c}(t)$ 属于 $\mathbb{Z}_p[[t-1]]$.

下面考虑所对应的群环. 现设 $n > 0$ 为正整数, 并考虑 Galois 群 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$. 以 σ_a 表示在自然同构 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n)^\times$ 下 $a \in (\mathbb{Z}/p^n)^\times$ 所对应的元. 考虑由群环 $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})]$ 到 $\mathbb{Z}_p[t]/(t^{p^n-1})$ 的 $\mathbb{Z}_p$ 模同态

$$\begin{gathered}\Phi_n : \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})] \to \mathbb{Z}_p[t]/(t^{p^n} - 1) \\ \sum \alpha_a \sigma_a \mapsto \sum \alpha_a t^a \quad (\alpha_a \in \mathbb{Z}_p).\end{gathered}$$

应注意, Φ_n 并不是环同态. Φ_n 为单射, 其像为这些 t^a(a 与 p 互素) 生成的 $\mathbb{Z}_p$ 子模.

考虑 Φ_n 的逆极限. 由引理 10.11, 因为 $\varprojlim \mathbb{Z}_p[t]/(t^{p^n} - 1) = \mathbb{Z}_p[[t-1]]$, 故得到

$$\Phi : \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]] \to \mathbb{Z}_p[[t-1]].$$

将 $\mathbb{Z}_p[[t-1]]$ 看作是 $\mathbb{Z}_p[[t^p-1]]$ 模, 则知其为以 $1, t, t^2, \cdots, t^{p-1}$ 为基底的自由模. 于是考虑 $\mathbb{Z}_p[[t-1]]$ 的子模 $H = \bigoplus_{a=1}^{p-1} t^a \mathbb{Z}_p[[t^p-1]]$, 则知 Φ 的像与 H 一致. 因此 Φ 给出了 $\mathbb{Z}_p$ 模之间的一个同构:

$$\Phi : \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]] \xrightarrow{\sim} H.$$

记此映射的逆映射为

$$D_p : H \xrightarrow{\sim} \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]].$$

我们把这个 D_p 想成是 $\mathbb{C}$ 上变换 $D(\sum a_n t^n, s) = \sum a_n n^{-s}$ 的 p 进类比.

那么在此由于 $g_{r,c}(t) \in \mathbb{Z}_p[[t-1]]$, 而 $g_{r,c}(t) \notin H$, 我们要对 $g_{r,c}(t)$ 进行修正使其属于 H. 令

$$f_{1,c}(t) = g_{1,c}(t) - g_{1,c}(t^p),$$

由 $g_{1,c}(t) = g_1(t) - cg_1(t^c)$, 则有

$$f_{1,c}(t) = g_1(t) - g_1(t^p) - c(g_1(t^c) - g_1(t^{cp})).$$

其中因为 $g_1(t)-g_1(t^p)$, $g_1(t^c)-g_1(t^{cp})$ 都在 $\dfrac{1}{t^p-1}H$ 之中, 故 $f_{1,c}(t)$ 在 H 之中. 我们定义元 θ_c 为

$$\theta_c = D_p(f_{1,c}(t)) \in \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/Q)]].$$

设 κ 为 (e) 小节所定义的分圆特征.

引理 10.15

(1) 设 $\mathbf{1}$ 为平凡特征, 它在群环上的延拓仍记为 $\mathbf{1}$. 此时有下面的交换图表. 其中斜的映射为根据以 1 代入 t 所定义的映射.

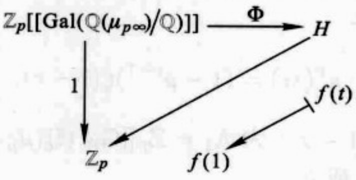
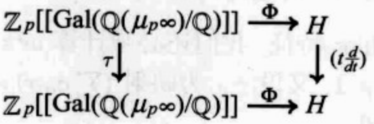


图 10.1

(2) 设 κ 为分圆特征, 定义 $\mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$ 的自同态 τ 为

$$\tau : \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]] \to \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$$
$$\left(\sum a_\sigma \sigma\right) \mapsto \left(\sum a_\sigma \kappa(\sigma)\sigma\right),$$

则 τ 是个自同构且有下面的交换图表:



其中 $\left(t\dfrac{d}{dt}\right)$ 是将 $f(t)$ 映到 $t\dfrac{d}{dt}f(t)$ 的映射, 它将 H 中的元映到 H 中的元. □

因为引理 10.15 的证明是简单的, 故而省略.

根据引理 10.15, 对于任意正整数 $r>0$ 我们可以进行如下的计算:

$$\begin{aligned}\kappa^{r-1}(\theta_c) &= \mathbf{1}(\tau^{r-1}(\theta_c))\\ &= \left(t\frac{d}{dt}\right)^{r-1} f_{1,c}(t)|_{t=1}\\ &= g_{r,c}(1) - p^{r-1}g_{r,c}(1)\\ &= (1-p^{r-1})g_{r,c}(1).\end{aligned}$$

将其与 Euler 的公式

$$(1-c^r)\zeta(1-r) = g_{r,c}(1)$$

相比较, 那么 Euler 的公式说的是, 被解析延拓到 $\mathbb{C}$ 的全纯函数 $D(g_{1,c}(t),s)$ 在 $1-r$ 的值即为 $g_{r,c}(1)$, 对应地, 我们能够把上面的公式想成 "被 p 进解析延拓到 Galois 群上的" $\theta_c = D_p(f_{1,c}(t))$ 在 κ^{r-1} 的值大体上就是 $g_{r,c}(1)$. 进一步比较两者得到了

$$\kappa^{r-1}(\theta_c) = (1-c^r)(1-p^{r-1})\zeta(1-r).$$

引理 10.16　设 τ 为引理 10.15(2) 中的那样, 并令 $\theta_c' = \tau^{-1}(\theta_c)$. 又设 σ_c 为使得 $\kappa(\sigma_c)=c$ 的 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ 中的元. 此时令 $z_1 = \dfrac{\theta_c'}{1-\sigma_c}$, 则 z_1 不依赖于 c 的选取, 并属于 $\Lambda_1^{\sim} = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]^{\sim}$. (对于 $\Lambda_1^{\sim}$ 的定义请见 (e) 小节.) 进而, 对于任意的正整数 $r>0$ 成立

$$\kappa^r(z_1) = (1-p^{r-1})\zeta(1-r).$$

[证明]　设 $z_{1,c} = \theta_c'/(1-\sigma_c)$ 为 $\Lambda_1 = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$ 的全商环 $Q(\Lambda_1)$ 的元, 那么对于所有正整数 r 成立

$$\begin{aligned}\kappa^r(z_{1,c}) &= \kappa^{r-1}(\theta_c)(1-c^r)^{-1}\\ &= (1-p^{r-1})\zeta(1-r).\end{aligned}$$

这里, 我们注意到由迄今所得到的事实可知这个等式给出了 $z_{1,c}$ 的特征刻画. 因为右端是个不依赖于 c 的表达式, 故而 $z_{1,c}$ 也不依赖于 c. 记 $z_1 = z_{1,c}$. 对于满足定义条件的任意 c 有 $(1-\sigma_c)z_1 \in \Lambda_1 = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$. 由于集合 $\{c \mid c$为与 p 互素的不小于 2 的整数$\}$ 在 $\mathbb{Z}_p^\times$ 中稠密, 故对于任意的 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ 有 $(1-\sigma)z_1 \in \Lambda_1$. 于是, 由 $\Lambda_1^{\sim}$ 的定义知有 $z_1 \in \Lambda_1^{\sim}$ ∎

以下设 ω 为 Teichmüller 特征, 我们还必须计算 $\omega^i\kappa^r(z_1)$ 的值. 首先设 p 为奇素数. 并设 i 为整数且 $\omega^i \neq \mathbf{1}$. 又设 τ_{ω^i} 为映射 $(\sum a_\sigma \sigma) \mapsto (\sum a_\sigma \omega^i(\sigma)\sigma)$, 我们从定义来计算 $\Phi(\tau_{\omega^i}\tau(z_1))$, 则知

$$\Phi(\tau_{\omega^i}\tau(z_1)) = \frac{\sum\limits_{a=1}^{p-1}\omega^i(a)t^a}{1-t^p}.$$

于是依照引理 10.15 得出

$$\omega^i\kappa^r(z_1) = \left(t\frac{d}{dt}\right)^{r-1}\left.\left(\frac{\sum\limits_{a=1}^{p-1}\omega^i(a)t^a}{1-t^p}\right)\right|_{t=1},$$

而右端按照像 $\zeta(1-r)$ 同样的解析延拓, 知其等于 $L(1-r,\omega^i)$. 这就是要求的表达式. 当 $p=2$ 时也有 $\Phi(\tau_\omega\tau(z_1)) = \sum\limits_{a=1}^{4}\omega(a)t^a/(1-t^4)$, 而其他的证明相同.

以上, 定理 10.14 得证.

最后对 $L_p(s,\mathbf{1})$ 在 $s=1$ 为具有留数 $1-\dfrac{1}{p}$ 的一阶极点进行证明. 在上面的证明中, 我们取了 $c\equiv 1 \pmod p$. 于是可写成

$$\begin{aligned} g_{1,c}(t) &= \left(t\frac{d}{dt}\right)\log\frac{1-t^c}{1-t} \\ &= \left(t\frac{d}{dt}\right)\log(1+t+\cdots+t^{c-1}), \end{aligned}$$

而因为 $1+t+\cdots+t^{c-1}\equiv 1 \pmod{(p,t-1)}$, 并代入形式幂级数 $\log(1+z)=\sum_{n=1}^{\infty}(-1)^{n-1}z^n/n$, 则可以将 $\log(1+t+\cdots+t^{c-1})$ 想成是 $\mathbb{Q}_p[[t-1]]$ 中的元. 同样地, 有

$$f_{1,c}(t)=\left(t\frac{d}{dt}\right)\left(\log\frac{1-t^c}{1-t}-\frac{1}{p}\log\frac{1-t^{cp}}{1-t^p}\right).$$

到此, 我们已证明了

$$\log\frac{1-t^c}{1-t}-\frac{1}{p}\log\frac{1-t^{cp}}{1-t^p}\in\mathbb{Z}_p[[t-1]].$$

这个元还在 H 之中. 根据引理 10.15, 有

$$\mathbf{1}(\theta_c')=(\log c)\left(1-\frac{1}{p}\right).$$

现在, 像在 (e) 小节那样分解 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})=\Delta\times\Gamma$, 并设 γ 为所取的 Γ 的拓扑生成元. 又设 $\{c_n\}$ 为收敛于 $\kappa(\gamma)$ 的正整数序列 ($\lim\limits_{n\to\infty}c_n=\kappa(\gamma)$), 并定义 $\theta_\gamma'=\lim\limits_{n\to\infty}\theta_{c_n}$, 由连续性得到

$$\mathbf{1}(\theta_\gamma')=(\log\kappa(\gamma))\left(1-\frac{1}{p}\right).$$

我们在此使用与 (e) 小节定理 10.6 和定理 10.7 的证明中所使用的相同记号. 设 $g_1(T)\in\dfrac{1}{T}\mathbb{Z}_p[[T]]$ 为由 z_1 按照 Δ 的平凡特征 $\mathbf{1}$ 所得到的幂级数 (若使用 (e) 中的记号, 则 $g_1(T)=\phi_{\mathbf{1},\kappa(\gamma)}(z_1)$). 由 $g_1(T)$ 的定义, 并由 $\mathbf{1}(\theta_\gamma')=(\log\kappa(\gamma))\left(1-\dfrac{1}{p}\right)$, $z_1=\theta_\gamma'/(1-\gamma)$, 可将 $g_1(T)$ 写成

$$g_1(T)=\frac{-\log\kappa(\gamma)}{T}\left(1-\frac{1}{p}\right)+\sum_{n=0}^{\infty}A_nT^n,\ A_n\in\mathbb{Z}_p.$$

如在 (e) 小节所见, 因为 $L_p(s,\mathbf{1})=g_1(\kappa(\gamma)^{1-s}-1)$, 故由上面推导出了

$$L_p(s,\mathbf{1})=\frac{1}{s-1}\left(1-\frac{1}{p}\right)+\sum_{n=0}^{\infty}a_n(s-1)^n.$$

这就完成了定理 10.6(2) 的证明.

(g) Ferrero-Washington 定理的证明

在此 (g) 小节中我们将证明定理 10.9. 我们建议读者在第一次阅读时, 先把这一节跳过直接进入 §10.2. 在此所给出的证明基于了 Sinnott 的想法, 这里与 (e) 一样也考虑 $N_0 = 1$ 的情形. 对一般的情形的证明是相同的.

[定理 10.9 的证明] 设 ω 为 Teichmüller 特征, 我们的目的是, 对于满足 $\omega^i \neq 1$ 的偶数 i 证明 $\frac{1}{2}G_{\omega^i}(T) \not\equiv 0 \pmod p$. 由我们的假定, 只要取 p 为奇素数即可. 于是, 要证明的是 $G_{\omega^i}(T) \not\equiv 0 \pmod p$. 我们仍然沿用 (e),(f) 小节的记号. 当设

$$\phi_{\omega^i,u} : \Lambda_1^{\sim} \to \mathbb{Z}_p[[T]]$$

为 (e) 中所给出的映射时, 我们想起了曾定义过 $G_{\omega^i}(T)$ 为

$$\phi_{\omega^i,u}(z_1) = g_{\omega^i}(T), \quad g_{\omega^i}(u(1+T)^{-1}-1) = G_{\omega^i}(T).$$

另外在 (f) 中 z_1 的构成是

$$z_1 = \frac{\tau^{-1}D_p(f_{1,c}(t))}{1-\sigma_c}.$$

为简单起见, 下面我们取 $c = 2$. 对于 $\mathbb{Z}_p^\times$ 的任意元 a, 定义 $\langle a\rangle \in 1 + p\mathbb{Z}_p$ 为 $\langle a\rangle = a/\omega(a)$. 因此 $a \in \mathbb{Z}_p^\times$ 有以下分解:

$$a = \omega(a)\langle a\rangle, \quad \omega(a) : \mathbb{Z}_p^\times \text{中的 } p-1 \text{ 次单位根},$$
$$\langle a\rangle \in 1 + p\mathbb{Z}_p.$$

设 u 为 $1 + p\mathbb{Z}_p$ 的一个固定的生成元, 我们记关于 u 的对数为 $\log_u : 1 + p\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_p$. 根据 ϕ_{ω^i} 的定义有

$$\phi_{\omega^i,u}(1-\sigma_2) = 1 - \omega(2)^i(1+T)^{\log_u\langle 2\rangle}.$$

由于 $\log_u\langle 2\rangle \neq 0$ 有 $\phi_{\omega^i,u}(1-\sigma_2) \not\equiv 0 \pmod p$, 那么要证明定理 10.9 只要证明

$$\phi_{\omega^i,u}(\tau^{-1}D_p f_{1,2}(t)) \not\equiv 0 \pmod p$$

即可. 考虑 $\phi_{\omega^i,u}(\tau^{-1}D_p f_{1,2}(t)) \equiv \phi_{\omega^{i-1},u}(D_p f_{1,2}(t)) \pmod p$, 并令

$$F_{1,2}(T) = \phi_{\omega^{i-1},u}(D_p f_{1,2}(t)) \in \mathbb{Z}_p[[T]].$$

下面我们证明 $F_{1,2}(T) \not\equiv 0 \pmod p$. 由

$$f_{1,2}(t) = \left(\sum_{a=1}^{p-1}(-1)^{a+1}t^a\right) \Big/ 1 + t^p$$
$$= \left(\sum_{\substack{a=1 \\ p\nmid a}}^{p^n}(-1)^{a+1}t^a\right) \Big/ 1 + t^{p^n},$$

我们有

$$F_{1,2}(T) \mod (1+T)^{p^{n-1}} - 1 = \frac{1}{2}\sum_{\substack{a=1 \\ p\nmid a}}^{p^n}(-1)^{a+1}\omega^{i-1}(a)(1+T)^{\log_u\langle a\rangle}$$
$$\in \mathbb{Z}_p[T]/((1+T)^{p^{n-1}}-1) \simeq \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}(\mu_p))].$$

现在来考虑 $F_{1,2}(T) \mod (p,(1+T)^{p^{n-1}}-1) \in \mathbb{F}_p[T]/((1+T)^{p^{n-1}}-1) = \mathbb{F}_p[T]/(T^{p^{n-1}})$. 由于有

$$F_{1,2}(T) \mod (p,(1+T)^{p^{n-1}}-1) = 0$$
$$\Longleftrightarrow \text{对于任意的 } \alpha \in \mathbb{Z}/p^{n-1}$$
$$\sum_{\substack{\log_u\langle a\rangle = \alpha (\bmod p^{n-1}) \\ a=1, p\nmid a}}^{p^n} (-1)^{a+1}\omega^{i-1}(a) = 0$$
$$\Longleftrightarrow \text{对于任意的 } \alpha \in (1+p\mathbb{Z})/(1+p^n\mathbb{Z}) \subset (\mathbb{Z}/p^n)^\times$$
$$\sum_{\substack{\langle a\rangle = \alpha \pmod{p^n} \\ a=1, p\nmid a}}^{p^n} (-1)^{a+1}\omega^{i-1}(a) = 0,$$

故将 $F_{1,2}(T) \mod (1+T)^{p^{n-1}} - 1$ 右端的 $\log_u\langle a\rangle$ 置换为 $(\langle a\rangle - 1)/p$ 即可. 最后令

$$\varphi_n(T) = \frac{1}{2}\sum_{\substack{a=1 \\ p\nmid a}}^{p^n}(-1)^{a+1}\omega^{i-1}(a)(1+T)^{\frac{\langle a\rangle - 1}{p}} \in \mathbb{F}_p[T]/(T^{p^{n-1}}),$$

于是有

$$F_{1,2}(T) \mod (p,(1+T)^{p^{n-1}}-1) \neq 0 \Longleftrightarrow \varphi_n(T) \neq 0.$$

因此令 $\varphi(T) = \lim\limits_{n\to\infty}\varphi_n(T) \in \mathbb{F}_p[[T]]$, 则只要证明 $\varphi(T) \neq 0$ 即可. 由于如果能断言 $(1+T)\varphi(T^p) \neq 0$, 那么当令

$$\psi_n(T) = \frac{1}{2}\sum_{\substack{a=1 \\ p\nmid a}}^{p^n}(-1)^{a+1}\omega^{i-1}(a)(1+T)^{\langle a\rangle} \in \mathbb{F}_p[[T]],\ \psi = \lim_{n\to\infty}\psi_n(T)$$

时, 变为了证明 $\psi \neq 0$ 就可以了. 现在令

$$H_a(T) = \frac{(-1)^{a+1}\omega^{i-1}(a)(1+T)^a}{1+(1+T)^p} \in \mathbb{F}_p(T),$$

则有

$$\psi = \sum_{a=1}^{p-1} H_a\left((1+T)^{\frac{1}{\omega(a)}} - 1\right) \in \mathbb{F}_p[[T]].$$

现在, 假设 $\psi = 0$. 因为 $i-1$ 为奇数, 注意有 $\omega^{i-1}(p-a) = -\omega^{i-1}(a)$, 那么利用下面的引理 10.17 则会有

$$H_a(T) + H_{p-a}\Big((1+T)^{-1} - 1\Big) = 2 \cdot H_a(T) \in \mathbb{F}_p,$$

从而导出矛盾. 于是 $\psi \neq 0$. ∎

引理 10.17 设对于 $a = 1, 2, \cdots, p-1$ 给出了 $H_a(T) \in \mathbb{F}_p(T)$, 使得其满足

$$\sum_{a=1}^{p-1} H_a\Big((1+T)^{\frac{1}{\omega(a)}} - 1\Big) = 0,$$

则有 $H_a(T) + H_{p-a}((1+T)^{-1} - 1) \in \mathbb{F}_p$. □

为了证明引理 10.17, 我们需要下面的引理.

引理 10.18 (Sinnott) 设 k 为域, $X_1, \cdots, X_n, Z$ 为不定元, $\langle X_1, \cdots, X_n \rangle$ 为域 $k(X_1, \cdots, X_n)$ 的元 $X_1, \cdots, X_n$ 在 $k(X_1, \cdots, X_n)^\times$ 中生成的子群, $Y_1, \cdots, Y_m$ 为 $\langle X_1, \cdots, X_n \rangle$ 中的元, 其任两个元都是乘法独立的. 就是说, 对于整数 a, b, 有 $Y_i^a = Y_j^b$ $(i \neq j)$ 仅在 $a = b = 0$ 时成立. 现设有有理函数 $r_1(Z), \cdots, r_m(Z) \in k(Z)$ 满足

$$\sum_{a=1}^{m} r_a(Y_a) = 0,$$

则 $r_a(Y_a)$ 全为常数. 即 $r_a(\mathbb{Z}) \in k$. □

我们在承认引理 10.18 下来证明引理 10.17.(关于这些引理的证明参考了有关文献[①])

[引理 10.17 的证明] 将环 $\mathbb{Z}[\mu_{p-1}]$ 看作 $\mathbb{Z}$ 模, 取其基底 $e_1, \cdots, e_n$. 令 $X_i = (1+T)^{e_i}$, 则 $X_1, \cdots, X_n$ 在 $\mathbb{F}_p((T))$ 中为 $\mathbb{F}_p$ 代数无关. 令 $m = \dfrac{p-1}{2}$ 并取 $Y_1, \cdots, Y_m$ 为 $Y_1 = (1+T)^{\frac{1}{\omega(1)}}, \cdots, Y_m = (1+T)^{\frac{1}{\omega(m)}}$. 它们中任意两个都是乘法独立的. 取

$$r_a(Z) = H_a(Z-1) + H_{p-a}(Z^{-1} - 1),$$

并应用引理 10.18 则得出引理 10.17. ∎

[引理 10.18 的证明] 由于它完全是个纯粹的代数引理, 故仅予概略的叙述. 由于可取 k 充分大, 故可设 $k^\times$ 含有无限阶的元 t. 假设对于非常数的有理函数 $r_a(Z)$ 成立引理 10.18 的那样的关系. 令 m 为使这个关系成立的最小整数. 因为 $r_1(Z) \neq 0$, 故 $m \geqslant 2$. 记 $Y_a = \prod_{i=1}^{n} X_i^{\alpha_{ia}}$, $\alpha_{ia} \in \mathbb{Z}$. 因为 Y_1, Y_2 为乘法独立, 故可取 $\beta_1, \cdots, \beta_n \in \mathbb{Z}$

[①] W.Sinnott, On the μ-invariant of the Γ-transform of a rational function, *Invent.Math.* **75** (1984) pp.273-282.

使得满足

$$\sum_{i=1}^{n}\alpha_{i1}\beta_i=0,\quad \sum_{i=1}^{n}\alpha_{i2}\beta_i\neq 0.$$

令 $\delta_a=\sum_{i=1}^{n}\alpha_{ia}\beta_i$, 并以 $X_i t^{\beta_i}$ 替换 X_i, 则有

$$\sum_{a=1}^{m}r_a(Y_a t^{\delta_a})=0.$$

因此有

$$\sum_{a=2}^{m}r_a(Y_a)-r_a(Y_a t^{\delta_a})=0,$$

因为 $r_2(Y_2)-r_2(Y_2 t^{\delta_2})\notin k$, 故这与 m 的最小性相矛盾. ∎

§10.2 理想类群与分圆 $\mathbb{Z}_p$ 扩域

本节在 (a),(b),(c) 小节做的代数准备, 以及在 (d) 小节的类域论的复习之后, 我们将对分圆域的理想类群进行研究. 主要目标是证明分圆 $\mathbb{Z}_p$ 扩域的理想类群 (准确地说即 (e) 小节所定义的 X) 作为 Galois 群的群环的模是个有限生成扭模. 从这个事实出发可以定义在本章前言所说的代数 p 进 ζ.

(a) 幂级数与 λ,μ 不变量

设 R 为完备赋值环, π 为其极大理想的生成元, $k=R/(\pi)$ 为其剩余域. 在 (a) 与 (b) 小节中, 我们考虑单变量幂级数环 $A=R[[T]]$. 最基本的是下面的命题.

命题 10.19 (p 进 Weierstrass 预备定理) *设 $f\in A=R[[T]]$ 为 R 上非 0 的形式幂级数, 则它可以唯一地写为*

$$\begin{aligned}f=&\pi^{\mu}(T^{\lambda}+a_1T^{\lambda-1}+\cdots+a_{\lambda})u(T),\\ &\lambda,\mu\in\mathbb{Z}_{\geqslant 0},\ a_1,\cdots,a_{\lambda}\in\pi R,\ u(T)\in R[[T]]^{\times}.\end{aligned}$$ □

对于幂级数 $f\in R[[T]]$, 命题 10.19 中的 λ,μ 分别叫做 f 的 **λ 不变量** (λ-invariant) 和 **μ 不变量** (μ-invariant), 以 $\lambda(f),\mu(f)$ 表示. 称多项式 $T^{\lambda}+a_1T^{\lambda-1}+\cdots+a_{\lambda}$ 为 f 的**伴随多项式**.

[命题 10.19 的证明] 首先证明下面的断言.

断言 *设 n 为正整数. $f\in(R/\pi^n)[[T]]$ 为 R/π^n 上的幂级数, 若 $f \bmod \pi\neq 0$, 则 f 可唯一地写成*

$$\begin{aligned}&f=g_n(T)u_n(T),\\ &g_n(T)=T^{\lambda}+a_1^{(n)}T^{\lambda-1}+\cdots+a_{\lambda}^{(n)},\ a_i^{(n)}\in\pi(R/\pi^n)\\ &u_n(T)\in(R/\pi^n)[[T]]^{\times}.\end{aligned}$$

[断言的证明] 对 n 进行数学归纳法证明. 当 $n=1$ 时, $(R/\pi)[[T]]=k[[T]]$ 是以 (T) 为极大理想的离散赋值环. 因此, 由 $f=f \bmod \pi \neq 0$, 知可唯一地写为 $f=T^{\lambda}u_1(T)$, $u_1(T)\in k[[T]]^{\times}$. 故而此时的断言得证.

设对于 n 的断言成立, 来证明其对 $n+1$ 成立. 设

$$f\in (R/\pi^{n+1})[[T]],\ f \bmod \pi \neq 0.$$

依归纳假定, 按照断言可唯一地写为 $f \bmod \pi^n = g_n(T)u_n(T)$. 现在, 取 $\tilde{g}(T)=T^{\lambda}+\tilde{a}_1T^{\lambda-1}+\cdots+\tilde{a}_{\lambda}$, $\tilde{u}(T)\in(R/\pi^{n+1})[[T]]$ 使得 $\tilde{g}(T) \bmod \pi^n = g_n(T)$, $\tilde{u}(T) \bmod \pi^n=u_n(T)$. 因 $f\equiv \tilde{g}(T)\tilde{u}(T) \pmod{\pi^n}$, 故可写为 $f-\tilde{g}(T)\tilde{u}(T)=\pi^n c(T)$. 我们注意到, 因为 $u_n(T)$ 为可逆元故 $\tilde{u}(T)$ 也是可逆元, 记 $\tilde{u}(T)^{-1}c(T)=\sum\limits_{i=0}^{\infty}c_iT^i$. 令

$$\alpha(T)=\sum_{i=0}^{\lambda-1}c_iT^i,\quad \beta(T)=\left(\sum_{i=\lambda}^{\infty}c_iT^{i-\lambda}\right)\tilde{u}(T),$$

并定义

$$\begin{aligned} g_{n+1}(T)&=\tilde{g}(T)+\pi^n\alpha(T),\\ u_{n+1}(T)&=\tilde{u}(T)+\pi^n\beta(T). \end{aligned}$$

如果注意到 $\tilde{g}(T) \bmod \pi = T^{\lambda}$, 那么在 $(R/\pi^{n+1})[[T]]$ 中有

$$\pi^n(\alpha(T)\tilde{u}(T)+\beta(T)\tilde{g}(T))=\pi^n c(T),$$

因而, $f=g_{n+1}(T)u_{n+1}(T)$. 由于 $\alpha(T) \bmod \pi$, $\beta(T) \bmod \pi$ 被唯一地确定, 从而 $g_{n+1}(T)$, $u_{n+1}(T)$ 也被唯一地确定. ∎

返回命题 10.19 的证明. 设 $f=\sum\limits_{i=0}^{\infty}A_iT^i$, 并令 $\mu=\min\{v_R(A_i)\}_{i\geqslant 0}$. 其中的 v_R 是满足 $v_R(\pi)=1$ 的 R 的离散赋值. 令 $f_0=f/\pi^{\mu}$, 由于 $f_0 \bmod \pi\neq 0$, 故如像断言所述那样可写 $f_0 \bmod \pi^n=(T^{\lambda}+a_1^{(n)}T^{\lambda-1}+\cdots+a_{\lambda}^{(n)})u_n(T)$. 若令

$$\begin{aligned} a_i&=(a_i^{(n)})\in R=\varprojlim R/(\pi^n)\\ u(T)&=(u_n(T))\in R[[T]]=\varprojlim (R/\pi^n)[[T]], \end{aligned}$$

则得到 $f=\pi^{\mu}(T^{\lambda}+a_1T^{\lambda-1}+\cdots+a_{\lambda})u(T)$. 另外, 这个分解是唯一确定的. ∎

(b) 特征理想与行列式

设 $R, A=R[[T]]$ 如 (a) 小节的那样. 我们将在 (b) 小节中考察有限生成的扭 A 模 M, 并定义 M 的特征理想 $\mathrm{Char}\,(M)$. 另外还将叙述, 当 M 满足某些条件时, 这个理想由某个线性映射的特征多项式所生成.

设 B 为主理想整环, M 为有限生成扭 B 模, 由众所周知的分解因子理论, 我们可将 M 写成

$$M \simeq B/(a_1^{n_1}) \oplus \cdots \oplus B/(a_r^{n_r}),\ a_1, \cdots, a_r \text{为 } B \text{ 的不可约元}$$
$$n_1, \cdots, n_r \text{为正整数}.$$

我们想对于有限生成扭 A 模进行类似的考虑. 然而因为 A 显然不是主理想整环, 也不是 1 维的环, 故而原封不动的类比不成立.

先来进行定义的确认. 所谓 M 为有限生成扭 A 模是说, M 为有限生成 A 模, 且存在非零元 $f \in A$ 使得 $fM = 0$ 成立. 对于两个有限生成扭 A 模 M, N, 如果存在 A 同态 $\varphi : M \to N$, 其核及余核作为 R 模均具有有限长, 那么我们就说 M 与 N 为**伪同构**(pseudo-isomorphism), 以 $M \sim N$ 表示. 当 R 的剩余域 $k = R/(\pi)$ 为有限域时, M 与 N 为伪同构则是说存在 A 模的正合序列

$$0 \to (\text{有限}) \to M \xrightarrow{\varphi} N \to (\text{有限}) \to 0.$$

就是说, 所谓伪同构可以说成是忽略掉有限差异后的同构. 有限生成扭 A 模之间的伪同构是个等价关系 (证明省略). 与前面所写出的有限生成扭 B 模的定理做类比, 成立下面的命题.

命题 10.20 设 M 为有限生成扭 A 模, 则可将 M 写成

$$M \sim A/(f_1^{n_1}) \oplus \cdots \oplus A/(f_r^{n_r}),\ f_1, \cdots, f_r \text{为 } A \text{ 的不可约元},$$
$$n_1, \cdots, n_r \text{为正整数}.$$

其中的 $\sim$ 为上述的伪同构. $f_1^{n_1}, \cdots, f_r^{n_r}$ 除相差一个单位因子外被 M 唯一决定. □

由于这是一个纯代数定理, 我们不准备在此证明它. 主理想整环 B 上的有限生成扭模 M 具有标准形, 我们回忆下面的证明. 取 φ 为使

$$B^m \xrightarrow{\varphi} B^r \to M \to 0$$

为正合序列的 B 模同态, 设 φ 由矩阵 X 表出, 那么由初等变换 X 可变形为

$$\begin{pmatrix} a_1^{n_1} & & 0 \\ & \ddots & \\ 0 & & a_r^{n_r} \end{pmatrix}.$$

从而有了 $M \simeq B/(a_1^{n_1}) \oplus \cdots \oplus B/(a_r^{n_r})$. 在命题 10.20 的证明里也取了那样的 φ 使得

$$A^m \xrightarrow{\varphi} A^r \to M \to 0$$

是 A- 模正合列. 当考虑对应于 φ 的矩阵 X 时, 仅对 X 进行初等变换并不能得到像上面那样形式, 但如果允许一些对应于伪同构的形变的话, 则可将 X 变形为

$$\begin{pmatrix} f_1^{n_1} & & 0 \\ & \ddots & 0 \\ 0 & & f_r^{n_r} \end{pmatrix}.$$

这样一来, 命题 10.20 便得到证明. 有兴趣的读者可看岩泽理论的参考文献 [2] 的 §13.2.

定义 10.21 将有限生成扭 A 模 M 按定理 10.20 写为

$$M \sim A/(f_1^{n_1}) \oplus \cdots \oplus A/(f_r^{n_r})$$

时, 我们称由 $f = f_1^{n_1} \cdot \cdots \cdot f_r^{n_r}$ 生成的 A 的理想 $(f) = fA$ 为 M 的**特征理想** (characteristic ideal), 以 $\mathrm{Char}\,(M)$ 表示. 又进一步定义 M 的 λ **不变量** 与 μ **不变量** 分别为

$$\lambda(M) = \lambda(f)$$

$$\mu(M) = \mu(f), \quad f = \prod_{i=1}^{r} f_i^{n_i}.$$

有限生成扭 $A = R[[T]]$ 模 M 为 R 自由是说, 当将 M 看作 R 模时它是自由 R 模. □

当 $\mathbb{Z}$ 模 M 被表示为

$$M \simeq \mathbb{Z}/(p_1^{n_1}) \oplus \cdots \oplus Z/(p_r^{n_r}), \quad p_1, \cdots, p_r \text{为素数}$$

时, M 的阶为 $p_1^{n_1} \cdot \cdots \cdot p_r^{n_r}$. 于是可知有像表 10.4 这样的类比.

表 10.4

有限 $\mathbb{Z}$ 模	有限生成扭 A 模
阶数	$\mathrm{Char}\ (M)$

设 $f \in A$ 满足 $\mu(f) = 0$, 由命题 10.19 知, 可将 f 写为

$$f = (T^{\lambda} + a_1 T^{\lambda-1} + \cdots + a_{\lambda}) u(T), \ u(T) \in A^{\times},$$

故 $A/(f)$ 作为 R 模是个秩为 λ 的自由 R 模. $A/(\pi^n) = (R/\pi^n)[[T]]$ 自然是个扭 R 模.

命题 10.22 对于有限生成扭 A 模 M, 下面的断言等价:

(1) M 为 R 自由的.

(2) M 不具有有限长的非零 R 子模, 且 $\mu(M) = 0$.

当上面条件成立时, M 为 $\lambda(M)$ 秩的自由 R 模.

[证明] 由于 M 为有限生成扭 A 模, 那么由命题 10.20, 存在 A 模同态 φ 使得

$$\varphi: M \to A/(f_1^{n_1}) \oplus \cdots \oplus A/(f_r^{n_r}),$$

且 $\mathrm{Ker}(\varphi), \mathrm{Coker}(\varphi)$ 均为长度有限的 R 模.

假定 (1) 为真, M 当然不含有长度有限的非零 R 子模. 另外因为 $\mathrm{Coker}(\varphi)$ 为长度有限的 R 模, 当考虑到我们在命题 10.22 前所说的事实时, 便知有 $\mu(f_1^{n_1}) = \cdots = \mu(f_r^{n_r}) = 0$. 因此, $\mu(M) = 0$.

反之假定 (2) 为真, 因为 $\mu(M) = 0$ 故 $A/(f_1^{n_1}) \oplus \cdots \oplus A/(f_r^{n_r})$ 为 R 自由. 因此 φ 的像 $\varphi(M)$ 也为 R 自由, 再由于 M 不包含长度有限的非零 R 子模, 故 φ 为单射, 从而 $M \simeq \varphi(M)$ 也为 R 自由.

由于 $A/(f_i^{n_i})$ 为 $\lambda(f_i^{n_i})$ 秩的自由 R 模, 如果 M 满足上述条件, 那么 M 便是秩为 $\lambda(M) = \sum_{i=1}^{r} \lambda(f_i^{n_i})$ 的自由 R 模. ∎

在下面的命题中我们将叙述 R 自由的有限生成扭 A 模 M 的特征理想可由对应于 T 倍的线性映射的特征多项式生成.

命题 10.23 设 M 为有限生成的扭 A 模, 且是 R 自由的. 又令 $\lambda = \lambda(M)$. 就是说, M 作为 R 模是个 λ 秩的自由模.

(1) 当我们将 M 仅看成是 R 模时便以 M_0 记之. 考虑自由 A 模 $A \otimes_R M_0$, 并定义 A 模同态映射

$$\Phi: A \otimes_R M_0 \to A \otimes_R M_0$$

为

$$\Phi(a \otimes m) = (Ta) \otimes m - a \otimes (Tm).$$

于是

$$0 \to A \otimes_R M_0 \xrightarrow{\Phi} A \otimes_R M_0 \xrightarrow{\psi} M \to 0$$

为 A 模的正合序列. 其中, ψ 是由 $\psi(a \otimes m) = am$ 定义的 A 模同态映射.

(2) A 同态映射 Φ 可表示为 λ 阶矩阵 $C \in M_\lambda(A)$. M 的特征理想 $\mathrm{Char}\,(M)$ 由 C 的行列式 $\det C$ 生成. 也就是说有

$$\mathrm{Char}\,(M) = (\det C) \subset A.$$

(3) T 倍映射 $T: M \to M$ $(x \mapsto Tx)$ 是将 M 看作自由 R 模时的 R 模同态映射, 并以 λ 阶矩阵 $V_T \in M_\lambda(R)$ 表示. 设 $C \in M_\lambda(A)$ 为 (2) 中那样, 那么 $\det C$ 等于 V_T 的特征多项式. 也就是说

$$\det C = \det(TI - V_T).$$

这里的 I 是 λ 阶单位矩阵.

(4) $\mathrm{Char}\,(M) = (\det(TI - V_T))$ □

(c) 命题 10.23 的证明

我们将在此证明命题 10.23, 由于这是个纯粹的代数定理, 没有兴趣的读者可以跳过这里先向前进.

先证明 (1). ψ 为满射是显然的. 另外, $\psi \circ \Phi = 0$ 也可立即明白. 因此要证明 $\mathrm{Ker}\psi \subset \mathrm{Im}\Phi$. 我们来证明比这个更强的下面的断言.

断言 对于任意的 $y \in A \otimes_R M_0$ 有

$$y - 1 \otimes \psi(y) \in \mathrm{Im}\Phi.$$

[证明] 要证明此断言只要对于形如 $y = T^n \otimes m$ ($n \in \mathbb{Z}_{\geqslant 0}$, $m \in M_0$) 的元证明就够了. 我们以对 n 的数学归纳法来证明该论断.

$n = 0$ 时, 由于 $y - 1 \otimes \psi(y) = 0$, 断言显然成立. 设其对于 n 成立, 我们来证明断言对于 $n+1$ 也成立. 由归纳假设知, 对于 $T^n \otimes Tm$, 存在 $z' \in A \otimes_R M_0$ 使得

$$T^n \otimes Tm - 1 \otimes T^{n+1}m = \Phi(z').$$

那么令 $z = T^n \otimes m + z'$, 则有

$$\begin{aligned}\Phi(z) &= T^{n+1} \otimes m - T^n \otimes Tm + T^n \otimes Tm - 1 \otimes T^{n+1}m \\ &= T^{n+1} \otimes m - 1 \otimes T^{n+1}m,\end{aligned}$$

于是对于 $y = T^{n+1} \otimes m$ 断言得证, 从而对于任意的 y 断言得到了证明. ∎

最后来证明 Φ 为单射. 设 F 为 A 的商域. 由于 M 为有限生成的扭 A 模, 故 $F \otimes_A M = 0$. 因此, 由 $A \otimes_R M_0 \xrightarrow{\Phi} A \otimes_R M_0 \to M \to 0$ 为正合序列, 得

$$1 \otimes \Phi : F \otimes_A A \otimes_R M_0 \to F \otimes_A A \otimes_R \otimes M_0$$

为满射. $F \otimes_A A \otimes_R M_0 = F \otimes_R M_0$ 是个 λ 维的 F 向量空间, $1 \otimes \Phi$ 是 F 向量空间之间的线性映射, 故是个单射. 由于自然映射 $A \otimes_R M_0 \to F \otimes_A A \otimes_R M_0$ ($a \otimes m \mapsto 1 \otimes a \otimes m$) 为单射, 故 Φ 为单射. 以上证明了 (1).

取 $e_1, \cdots, e_\lambda$ 为 R 模 M_0 的一组基底. 那么 $A \otimes_R M_0$ 便是以 $1 \otimes e_1, \cdots, 1 \otimes e_\lambda$ 为一组基底的自由 A 模. 因此, A 同态映射 Φ 在这组基底下可用 λ 阶矩阵 $C \in M_\lambda(A)$ 表示. 因为从 M_0 到 M_0 的映射 $x \mapsto Tx$ 为 R 模同态, 故也可用关于基底 $e_1, \cdots, e_\lambda$ 的矩阵 $V_T \in M_\lambda(R)$ 表示. 由于有

$$\begin{aligned}\Phi(1 \otimes e_i) &= T \otimes e_i - 1 \otimes Te_i \\ &= (1 \otimes e_i)T - (1 \otimes e_i)V_T,\end{aligned}$$

若设 I 为 λ 阶单位矩阵, 则有 $C = TI - V_T$, 从而 $\det C = \det(TI - V_T)$. 因此 (3) 得证. 注意, 因为 $\det(TI - V_T)$ 中 T^λ 的系数为 1, 故 $\mu(\det C) = 0$.

设 K 为 R 的商域, 考虑 $K\otimes_R M$. 由命题 10.20 记

$$M\sim A/(f_1^{n_1})\oplus\cdots\oplus A/(f_r^{n_r}).$$

于是得到了同构

$$K\otimes_R M\simeq(K\otimes_R A)/(f_1^{n_1})\oplus\cdots\oplus(K\otimes_R A)/(f_r^{n_r}).$$

记其右端为 N_k, 并比较下面两个正合序列

$$\begin{array}{ccccccccc} 0\to & K\otimes_R A\otimes_R M_0 & \xrightarrow{1\otimes\Phi} & K\otimes_R A\otimes_R M_0 & \to & K\otimes_R M & \to 0 \\ & & & & & \wr\vert & \\ 0\to & (K\otimes_R A)^r & \xrightarrow{\Phi'} & (K\otimes_R A)^r & \to & N_k & \to 0 \end{array}$$

$$\Phi'(x_1,\cdots,x_r)=(f_1^{n_1}x_1,\cdots,f_r^{n_r}x_r)$$

则知 $\det C$ 与 $\det\Phi'=\prod\limits_{i=1}^r f_i^{n_i}$ 仅仅差一个 $(K\otimes_R A)^\times$ 的元 (注意, $K\otimes_R A=A[1/\pi]$ 为主理想整环). 因此由假定并根据命题 10.22 得到 $\mu(M)=0$, 从而 $\mu(\prod\limits_{i=1}^r f_i^{n_i})=0$. 这样, $\det C$ 与 $\prod\limits_{i=1}^r f_i^{n_i}$ 均不被 π 除尽. 从而两者仅仅差一个 $A^\times$ 的元, 于是生成 A 中同一个理想. 所以有

$$\mathrm{Char}(M)=\left(\prod_{i=1}^r f_i^{n_i}\right)=(\det C).$$

(2) 得证.

(2) 与 (3) 合在一起便得到了 (4).

(d) 最大非分歧 Abel 扩域与理想类群

这里是为下面的 (e) 小节做准备, 对于非分歧类域论进行复习, 做些必要的小结.

设 K 为有理数域 $\mathbb{Q}$ 的有限扩域, 为简单起见我们设其没有实素点. 称使所有素理想均为非分歧的扩域为**非分歧扩域**. 设 L/K 为在 K 的代数闭包 $\overline{K}$ 中最大的非分歧的 Abel 扩域, 像在 §8.1(g) 的 (三) 中所叙述的那样, L/K 为有限扩域, 与理想类群 $Cl(K)$ 之间存在同构

$$\Phi_K: Cl(K)\xrightarrow{\sim}\mathrm{Gal}\,(L/K).$$

设 $\boldsymbol{p}$ 为 K 的素理想, $[\boldsymbol{p}]$ 为 $Cl(K)$ 中 $\boldsymbol{p}$ 的类, 而 Φ_K 是满足

$$\Phi_K([\boldsymbol{p}])=\mathrm{Frob}_{\boldsymbol{p}}\in\mathrm{Gal}\,(L/K)$$

的映射. 这里的 $\mathrm{Frob}_{\boldsymbol{p}}$ 为 $\boldsymbol{p}$ 的 Frobenius 置换. 称 Φ_K 为互反映射, 而称 L 为 K 的绝对类域.

那么, 现在设 K/F 为有限 Galois 扩域. Galois 群 $\mathrm{Gal}(K/F)$ 以

$$\sigma([\boldsymbol{a}]) = [\sigma(\boldsymbol{a})],\ \sigma \in \mathrm{Gal}(K/F)$$

自然地作用在理想类群 $Cl(K)$ 上. 这里的 $[\boldsymbol{a}]$ 表示理想 $\boldsymbol{a}$ 在 $Cl(K)$ 中的类. 另外, L/F 也是个 Galois 扩域. 之所以这样说是因为, 如果设 L' 为 L 在 F 上的共轭域, 那么由于 K/F 为 Galois 扩域, 故 L' 包含了 K. 现在 L'/K 是个非分歧扩域, 又因为 L/K 与 L'/K 的 Galois 群同构, 故 L'/K 也是 Abel 扩域. 可是, L 是最大的非分歧扩域, 从而 $L' \subset L$. 因此 L/F 是 Galois 扩域.

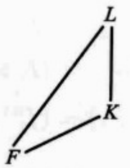


图 10.2

下面, 按照共轭定义 $\mathrm{Gal}(K/F)$ 在 $\mathrm{Gal}(L/K)$ 上的作用. 也就是说, 对于 $\sigma \in \mathrm{Gal}(K/F)$, $s \in \mathrm{Gal}(L/K)$, 定义

$$\sigma(s) = \tilde{\sigma}s\tilde{\sigma}^{-1}.$$

这里的 $\tilde{\sigma}$ 是 σ 在 $\mathrm{Gal}(L/F)$ 的延拓 (即满足 $\tilde{\sigma}|_K = \sigma$ 的元). 由于 $\mathrm{Gal}(L/K)$ 为 Abel 群, 故 $\tilde{\sigma}s\tilde{\sigma}^{-1}$ 不依赖于 $\tilde{\sigma}$ 的选取. 对于 Frobenius 置换, 由于成立

$$\mathrm{Frob}_{\sigma(\boldsymbol{p})} = \tilde{\sigma}\mathrm{Frob}_{\boldsymbol{p}}\tilde{\sigma}^{-1},\ \sigma \in \mathrm{Gal}(K/F),$$

于是知道互反映射 $\Phi_K : Cl(K) \to \mathrm{Gal}(L/K)$ 与 Galois 群的作用可交换. 即成立

$$\Phi_K([\sigma(\boldsymbol{a})]) = \sigma\Phi_K([\boldsymbol{a}]),\ \sigma \in \mathrm{Gal}(K/F).$$

在下面我们来叙述与范映射的交换性. 因为对于 K 的理想 $\boldsymbol{a}$, $\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\boldsymbol{a})$ 可以写为

$$\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\boldsymbol{a}) = \boldsymbol{b} \cdot O_K \quad (\boldsymbol{b}\text{为 } F \text{ 的理想}),$$

我们便称 F 的理想 $\boldsymbol{b}$ 为 $\boldsymbol{a}$ 的范, 并以 $N\boldsymbol{a}$ 表示. 进而按照定义

$$N([\boldsymbol{a}]) = [N\boldsymbol{a}]$$

来定义范映射

$$N : Cl(K) \to Cl(F).$$

现设 L'/F 为最大非分歧 Abel 扩域, 那么 $L'K$ 为 K 的非分歧 Abel 扩域, 故 $L'K \subset L$. 特别地, 因为 $L' \subset L$, 故定义了自然映射

$$\begin{aligned} i : \mathrm{Gal}\,(L/K) \to &\ \ \mathrm{Gal}\,(L'/F) \\ \sigma \mapsto &\ \ \sigma|_{L'}, \end{aligned}$$

将其表示为 i. 这时存在以下的交换图表

$$\begin{array}{ccc} Cl(K) & \xrightarrow{\Phi_K} & \mathrm{Gal}(L/K) \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle i} \\ Cl(F) & \xrightarrow[\Phi_F]{} & \mathrm{Gal}(L'/K). \end{array}$$

在类域论那一章里, 对于由伊代尔类群到 Galois 群的互反映射, 曾证明过 N 与 i 可交换. 由此推导出上面图表的可交换性.

(e) 分圆 $\mathbb{Z}_p$ 扩域的理想类群

在此我们将叙述分圆 $\mathbb{Z}_p$ 扩域的理想类群作为群环上的模是个有限生成扭模.

与 §10.0 一样, 对于正整数 n 以 μ_n 表示 $\overline{\mathbb{Q}}$ 中的所有 n 次单位根. 设 K 为 $\mathbb{Q}$ 的有限扩域, 并假定

$$\begin{aligned} &\text{当 } p \text{ 为奇素数时}, \quad \mu_p \subset K \\ &\text{当 } p = 2 \text{ 时}, \qquad\quad \mu_4 \subset K. \end{aligned}$$

特别地, K 没有实素点.

对于正整数 n, 令

$$K_n = K(\mu_{p^n}), \quad K_\infty = \bigcup_{n>0} K_n.$$

与迄今为止所做过的一样, 我们定义

$$\kappa : \mathrm{Gal}\,(K_n/K) \hookrightarrow (\mathbb{Z}/p^n)^\times$$

如下: 对于 $\sigma \in \mathrm{Gal}\,(K_n/K)$, $\zeta \in \mu_{p^n}$ 使得 $\sigma(\zeta) = \zeta^{\kappa(\sigma)}$, $\kappa(\sigma) \in (\mathbb{Z}/p^n)^\times$, 但由以上假定有

$$\kappa(\sigma) \in (1 + 2p\mathbb{Z}_p)/p^n\mathbb{Z}_p \subset (\mathbb{Z}_p/p^n)^\times \subset (\mathbb{Z}/p^n)^\times.$$

还应注意, κ 是个单射. 因此定义了

$$\kappa : \mathrm{Gal}\,(K_n/K) \hookrightarrow (1 + 2p\mathbb{Z}_p)/p^n\mathbb{Z}_p \subset (\mathbb{Z}/p^n)^\times$$

取逆极限便得到了同态

$$\kappa : \mathrm{Gal}\,(K_\infty/K) \hookrightarrow 1 + 2p\mathbb{Z}_p \subset \mathbb{Z}_p^\times.$$

因为 $\mathbb{Q}(\mu_{p^n})$ 为 $\mathbb{Q}$ 的 $\varphi(p^n) = p^{n-1}(p-1)$ 次扩域, 故 $\mathbb{Q}(\mu_{p^\infty}) = \bigcup \mathbb{Q}(\mu_{p^n})$ 为 $\mathbb{Q}$ 的无限次扩域. 由于 K 为 $\mathbb{Q}$ 的有限扩域, 故 K_∞/K 为 K 的无限扩域. 特别地, $K_\infty \neq K$.

如同 §10.1(b) 所说过的那样, 由于 $1+2p\mathbb{Z}_p$ 同构于加法群 $\mathbb{Z}_p$, 并且 κ 为连续, 故而 $\mathrm{Gal}(K_\infty/K)$ 同构于 $\mathbb{Z}_p$ 的一个非零闭子群. 这样的群恰好是 $p^m\mathbb{Z}_p$ $(m \geqslant 0)$, 它们每个都同构于 $\mathbb{Z}_p$, 故而 $\mathrm{Gal}(K_\infty/K)$ 与 $\mathbb{Z}_p$ 同构. 令

$$\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p.$$

称扩域 K_∞/K 为**分圆 $\mathbb{Z}_p$ 扩域**.

设 $n \geqslant 0$ 为正整数. 以下我们将理想类群 $Cl(K_n)$ 的运算以加法表示, 单位元则以 0 表示. 设 A_{K_n} 为 $Cl(K_n)$ 的 p-Sylow 群. 于是 A_{K_n} 为 $Cl(K_n)$ 中所有具有 p 幂阶的元构成的子群. 又记 $Cl(K_n)$ 中所有阶与 p 互素的元构成的子群为 A'_{K_n}, 那么我们注意到有

$$Cl(K_n) = A_{K_n} \oplus A'_{K_n}.$$

称扩张次数为 p 的幂次的扩域为 p-扩域. 记 K_n 的非分歧 Abel p- 扩域中最大者为 L_n. 又记 K_n 的非分歧 Abel 扩域中最大者为 $\mathcal{L}_n$, 那么 $L_n \subset \mathcal{L}_n$. 另外, 根据类域论的互反映射可得到同构

$$\Phi_{K_n} : Cl(K_n) \xrightarrow{\sim} \mathrm{Gal}(\mathcal{L}_n/K_n)$$

(参看 (d) 小节). 设 L'_n 为 K_n 的扩张次数与 p 互素的非分歧 Abel 扩域中的最大者, 于是有

$$\mathrm{Gal}(\mathcal{L}_n/K_n) = \mathrm{Gal}(L_n/K_n) \times \mathrm{Gal}(L'_n/K_n).$$

将上面的两种表示进行比较, 由类域论的互反映射便得到了同构

$$\Phi_{K_n} : A_{K_n} \xrightarrow{\sim} \mathrm{Gal}(L_n/K_n).$$

考虑对于 $m > n$ 的范映射 $N : Cl(K_m) \to Cl(K_n)$, 有 $N(A_{K_m}) \subset A_{K_n}$. 于是定义了

$$N : A_{K_m} \to A_{K_n}.$$

另外, 我们以

$$\sigma \mapsto \sigma|_{L_n}$$

定义

$$i : \mathrm{Gal}(L_m/K_m) \to \mathrm{Gal}(L_n/K_n),$$

根据 (d) 小节所叙述过的事实我们得到了以下的交换图表:

$$\begin{array}{ccc} A_{K_m} & \xrightarrow{\Phi_{K_m}} & \mathrm{Gal}(L_m/K_m) \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle i} \\ A_{K_n} & \xrightarrow{\Phi_{K_n}} & \mathrm{Gal}(L_n/K_n). \end{array}$$

取 Φ_{K_n} 的逆极限. 令

$$X = \varprojlim_{\text{范映射}} A_{K_n}$$

$$L_\infty = \bigcup_{n\geqslant 0} L_n$$

(L_∞ 是 K_∞ 的所有非分歧 Abel p- 扩域的并). 因为 $\mathrm{Gal}\,(L_\infty/K_\infty) = \varprojlim \mathrm{Gal}\,(L_n/K_n)$, 故取 Φ_{K_n} 的逆极限则存在同构映射

$$\Phi : X \xrightarrow{\sim} \mathrm{Gal}\,(L_\infty/K_\infty).$$

如在 (d) 小节所说过的那样, Φ_{K_n} 与 $\mathrm{Gal}\,(K_n/K)$ 的作用可交换. 因此, Φ_{K_n} : $A_{K_n} \to \mathrm{Gal}\,(L_n/K_n)$ 是个 $\mathbb{Z}_p[\mathrm{Gal}\,(K_n/K)]$ 模同构映射. 所以, 上面的 Φ 是个 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K)]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$ 模同构映射. 总结以上, 我们有

命题 10.24 设 L_n 为 K_n 的最大非分歧 Abel p- 扩域, 令

$$L_\infty = \bigcup_{n\geqslant 0} L_n$$

$$X = \varprojlim_{\text{范映射}} A_{K_n}$$

$$\Lambda = \mathbb{Z}_p[[\Gamma]] = \mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K)]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}\,(K_n/K)],$$

则按照类域论的互反映射, 得到了 Λ 模同构映射

$$\Phi : X \xrightarrow{\sim} \mathrm{Gal}\,(L_\infty/K_\infty).$$ □

注意, 由于 Γ 与 $\mathbb{Z}_p$ 同构, 根据命题 10.10, $\Lambda = \mathbb{Z}_p[[\Gamma]]$ 同构于单变量的形式幂级数环 $\mathbb{Z}_p[[T]]$.

下面的定理是 §10.2 的主定理.

定理 10.25 (岩泽) $X = \varprojlim A_{K_n}$ 作为 $\Lambda = \mathbb{Z}_p[[\Gamma]] = \mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K)]]$ 模是个有限生成扭 Λ 模. □

根据这个定理, $\lambda(X), \mu(X)$ 以及 Λ 的理想 $\mathrm{Char}\,(X)$ 均有定义. 称 $\lambda(X), \mu(X)$ 分别为 K 的 λ 不变量和 μ 不变量. 这还使得我们可以将 $\mathrm{Char}\,(X)$ 的生成元考虑为 "代数的 p 进 ζ". 更准确的代数 p 进 ζ 的定义将在 §10.3(a) 中给出.

(f) 定理 10.25 的证明及其应用

在此我们将证明定理 10.25, 即证明 $X = \varprojlim A_{K_n}$ 为有限生成扭 Λ 模. 在判定为有限生成扭 Λ 模方面, 我们要用到下面的引理.

引理 10.26 设 m_Λ 为 Λ 的极大理想. M 为一个投射有限 Λ 模, 即有 $M = \varprojlim M_i$ (M_i 是有限 Λ 模) 这样的 Λ 模. 又设存在某个元 $f \in m_\Lambda$, 使得 M/fM 为有限 Λ 模, 于是 M 是个有限生成扭 Λ 模.

[证明] 因为 M/fM 为有限, 故 $M/m_\Lambda M$ 有限. 将 $M/m_\Lambda M$ 看为有限维 $\Lambda/m_\Lambda = \mathbb{F}_p$ 向量空间, 并取 $\overline{x_1}, \cdots, \overline{x_r}$ 为其生成元. 其中 $x_1, \cdots, x_r$ 为 M 中的元, 使得 $x_i \bmod m_\Lambda = \overline{x_i}$. 我们来证明 $x_1, \cdots, x_r$ 生成了 M. 记由 $x_1, \cdots, x_r$ 生成的 M 的 Λ 子模为 N. 设 $M = \varprojlim M_i$ (M_i 为有限 Λ 模), $\varphi_i : M \to M_i$ 为自然映射, 由于 M_i 为有限, 根据中山 (Nakayama) 引理知, M_i 由 $\varphi_i(x_1), \cdots, \varphi_i(x_r)$ 生成.

再有, $N = \Lambda x_1 + \cdots + \Lambda x_r$ 是紧群 Λ^r 的像, 故而也是紧的, 从而是完备的. 于是有 $N = \varprojlim \varphi_i(N) = \varprojlim M_i = M$, 因此 M 为有限生成.

下面我们假设 M 不是扭 Λ 模, 从而导出矛盾. 由假设, 有元 $x \in M$, 对于任何的 $a \in \Lambda - \{0\}$ 都有 $ax \neq 0$. 设 $\langle x \rangle$ 为 x 生成的 M 的子模, 并令 $M' = M/\langle x \rangle$. 因为 $\langle x \rangle / f\langle x \rangle \simeq \Lambda/f\Lambda$ 为无限群, 又考虑到 M/fM 为有限模, 则 $M'[f] = \{x \in M' \mid fx = 0\}$ 为无限群. 因此, M'/fM' 为有限, 而 $M'[f]$ 为无限. 现设 T 为 M' 的 Λ 扭元所构成的子 Λ 模, 于是 T/fT 为有限而 $T[f] = \{x \in T \mid fx = 0\}$ 为无限. 故而可以将命题 10.22 应用于有限生成模 T, 因为 T/fT 为有限推导出了 $T[f]$ 为有限, 从而得出了矛盾. ∎

那么, 在扩域 $\mathbb{Q}(\mu_{p^n})/\mathbb{Q}$ 上, p 以外的素数均非分歧. 因此, 在 K_∞/K 中的 p 之上的素理想中没有是非分歧的. 这又是因为 $\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p$ 为无限次完全分歧扩域, 故对于 $\mathbb{Q}_p$ 的有限扩域 k 而言, $k(\mu_{p^\infty})/k$ 也是分歧扩域. 因此, 在 K_∞/K 中, p 之上的素理想必定是分歧的.

一般地, 设 L/F 为数域的 (不一定限于有限次的)Galois 扩域, v 为 F 的一个素理想, w 为 v 之上在 L 的素理想. 并设 F_v, L_w 分别是 F, L 对于 v, w 的完备化, 这时, 按照 $\sigma \mapsto \sigma|_L$ 给出的映射可将 $\mathrm{Gal}\,(L_w/F_v)$ 看作是 $\mathrm{Gal}\,(L/F)$ 的子群. 称这个子群 $\mathrm{Gal}\,(L_w/F_v)$ 为在 w 的**分解群** (decomposition group). 记在 L_w 中 F_v 的最大非分歧扩域为 F'_v. 将 $\mathrm{Gal}\,(L_w/F'_v)$ 也看作 $\mathrm{Gal}\,(L/F)$ 的子群, 并称其为在 w 的**惯性群** (inertia group). 由定义, w 为非分歧等价于惯性群为平凡. L/F 为 Abel 扩域时, 在 w 的分解群和惯性群仅仅由 v 决定, 故而这时也称它们为在 v 的分解群和惯性群.

以 $\boldsymbol{p}_1, \cdots, \boldsymbol{p}_s$ 表示 p 之上的 K 的素理想. 我们记扩域 K_∞/K 在 $\boldsymbol{p}_i$ 的惯性群为 I_i, 那么按照上面所说, 由于 $\boldsymbol{p}_i$ 是分歧的, 故 $I_i \neq \{1\}$. 因此, 对于 $\Gamma = \mathrm{Gal}\,(K_\infty/K) \simeq \mathbb{Z}_p$, 可写为 $I_i = \Gamma^{p^{n_i}}$ (记 Γ 上的运算为乘法). 令 $I = \bigcap_{i=1}^{s} I_i$. 于是有

$$I = \Gamma^{p^M}, \ M = \max\{n_1, \cdots, n_s\}.$$

设对应于 I 的 K_∞/K 的中间域为 $K_N = K(\mu_{p^N})$. 就是说, 我们考虑使得

$$\mathrm{Gal}\,(K_\infty/K_N) = I$$

成立的域 K_N $(N \in \mathbb{Z}_{\geqslant 0})$. 这里的 N 是满足此关系的最大的整数.

对于 $n \geqslant N$, L_n/K_n 为非分歧, 而因为 K_∞/K_n 在 p 之上的所有素理想均为完全分歧, 故有

$$L_n \cap K_\infty = K_n.$$

因此有同构

$$A_{K_n} \simeq \mathrm{Gal}\,(L_n/K_n) \simeq \mathrm{Gal}\,(L_n \cdot K_\infty/K_\infty).$$

因为根据命题 10.24 有 $X \simeq \mathrm{Gal}\,(L_\infty/K_\infty)$, 从而有自然映射

$$X \to A_{K_n} \quad 为满射 \quad (n \geqslant N).$$

现令

$$Y = \mathrm{Ker}(X \to A_{K_N}).$$

引理 10.27 设 γ' 为 $\mathrm{Gal}\,(K_\infty/K_N)$ 作为 $\mathbb{Z}_p$ 模的生成元, 于是自然映射 $X \to A_{K_{N+1}}$ 诱导出同构

$$Y/(1+\gamma'+\cdots+(\gamma')^{p-1})Y \xrightarrow{\sim} \mathrm{Ker}(A_{K_{N+1}} \xrightarrow{\text{范映射}} A_{K_N}). \qquad \square$$

从引理 10.27 可直接推导出定理 10.25. 事实上, 上面同构的右端为有限, 故根据引理 10.26 知 Y 是有限生成扭 Λ 模. 另一方面, 由定义得知

$$X/Y \xrightarrow{\sim} A_{K_N}$$

为同构, 故而 X 与 Y 只有有限的差异, 从而 X 也是有限生成扭 Λ 模.

由于 $X/Y \xrightarrow{\sim} A_{K_N}$, 故要证明引理 10.27 只要证明以下的引理即可.

引理 10.28

$$\mathrm{Ker}(X \to A_{K_{N+1}}) = (1+\gamma'+\cdots+(\gamma')^{p-1})Y. \qquad \square$$

下面我们来证明引理 10.28. 在证明中我们本质上使用了类域论.

以 (d) 小节所说的方法知 L_∞/K_N 为 Galois 扩域. 现令

$$\mathcal{G} = \mathrm{Gal}\,(L_\infty/K_N).$$

由于根据命题 10.24 有 $X \xrightarrow{\sim} \mathrm{Gal}\,(L_\infty/K_\infty)$, 故我们将 X 与 $\mathrm{Gal}\,(L_\infty/K_\infty)$, 以及 Y 与 $\mathrm{Gal}\,(L_\infty/L_N K_\infty)$ 看成是一样的, 从而将 X, Y 都看作 $\mathcal{G}$ 的子群. 进一步再令

$$\Gamma_N = \mathrm{Gal}\,(K_\infty/K_N),\ \mathcal{H} = \mathrm{Gal}(L_\infty/L_N)$$

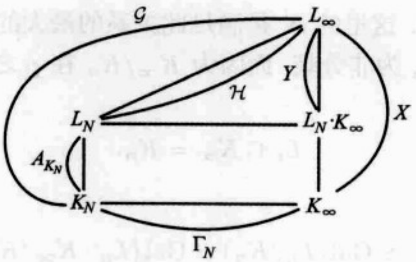


图 10.3

(参看图 10.3).

以 $\boldsymbol{q}_1, \cdots, \boldsymbol{q}_r$ 表示 p 之上的 K_N 的素理想. 取 $\boldsymbol{q}_i$ 之上在 L_∞ 中的一个素理想, 并记其在 L_∞/K_N 的惯性群为 J_i. 设

$$c : \mathcal{G} \to \Gamma_N$$

为自然的同态映射, 则有 $c(J_i) = \Gamma_N$. 另外还有 $\mathrm{Ker}(c) = X$, 并因为 L_∞/K_∞ 为非分歧扩域, 故有 $J_i \cap X = \{1\}$, 从而推导出 c 为同构 $J_i \xrightarrow{\sim} \Gamma_N$. 设 $\gamma_i \in J_i$ 为使 $c(\gamma_i) = \gamma'$ 的元, 那么 J_i 作为 $\mathbb{Z}_p$ 模由 γ_i 生成.

引理 10.29 *Y 由 $(\gamma'-1)X$ 和 $\gamma_i\gamma_1^{-1}$, $i = 1, \cdots, r$ (拓扑地) 生成.*

[证明]　因为 L_N 为 K_N 的最大非分歧 Abel p- 扩域, 故 $\mathcal{H}$ 等于以 $\mathcal{G}$ 的换位子群和 $J_1, \cdots, J_r$ 生成的 $\mathcal{G}$ 子群的 (拓扑) 闭包.

设 $\mathcal{G}'$ 为 $\mathcal{G}$ 的换位子群的 (拓扑) 闭包, 我们来证明

$$\mathcal{G}' = (\gamma' - 1)X.$$

回想一下, Γ_N 在 $X = \mathrm{Gal}\,(L_\infty/K_\infty)$ 上的作用是用共轭定义的, 那么对于 $\sigma \in X$, 由于 γ' 在 $\mathcal{G}$ 上的提升可取作 $\gamma_i \in J_i$, 故我们有

$$(\gamma' - 1)\sigma = \gamma_i \sigma \gamma_i^{-1} \sigma^{-1}.$$

因此 $(\gamma' - 1)X \subset \mathcal{G}'$. 另一方面, 因为 $c : \mathcal{G} \to \Gamma_N$ 诱导出了 $J_i \xrightarrow{\sim} \Gamma_N$, 故可写成 $\mathcal{G} = J_i X$. 现在

$$\gamma_i^a \sigma \gamma_i^{-a} \sigma^{-1} = ((\gamma')^a - 1)\sigma,\ \sigma \in X,\ a \in \mathbb{Z}_p,$$

由于 $\gamma' - 1$ 除尽 $(\gamma')^a - 1$, 那么应用 $\mathcal{G} = J_i X$ 便知道有 $\mathcal{G}' \subset (\gamma' - 1)X$.

设 $\varphi : \mathcal{G} \to \mathcal{G}/\mathcal{G}'$ 为自然映射, 于是 $\varphi(\mathcal{H})$ 由 $\varphi(J_1), \cdots, \varphi(J_r)$ 生成. 再注意到 $X = \mathrm{Ker}(c)$, 那么便知, 拓扑地 $\varphi(\mathcal{H} \cap X)$ 由 $\gamma_i\gamma_1^{-1}$, $i = 1, \cdots, r$ 生成. 由于 $\mathcal{G}' = (\gamma' - 1)X$, $\mathcal{H} \cap X$ 便由 $(\gamma' - 1)X$ 与 $\gamma_i\gamma_1^{-1}$, $i = 1, \cdots, r$ 生成. 因为 $Y = \mathcal{H} \cap X$, 故引理 10.29 得证.

∎

[引理 10.28 的证明] 若将引理 10.29 的证明应用到 $\mathrm{Ker}(X \to A_{K_{N+1}})$ 上, 则知此群由

$$((\gamma')^p - 1)X \text{ 与 } \gamma_i^p\gamma_1^{-p}\ (i = 1, \cdots, r)$$

生成. 现在由于有

$$\begin{aligned}(1+\gamma'+\cdots+(\gamma')^{p-1})(\gamma'-1)X &= ((\gamma')^p-1)X\\ (1+\gamma'+\cdots+(\gamma')^{p-1})(\gamma_i\gamma_1^{-1}) &= \gamma_i\gamma_1^{-1}\cdot\gamma_1\gamma_i\gamma_1^{-1}\gamma_1^{-1}\gamma_1^2\gamma_i\gamma_1^{-1}\gamma_1^{-2}\cdot\\ &\quad\cdots\cdot\gamma_1^{p-1}\gamma_i\gamma_1^{-1}\gamma_1^{-(p-1)}\\ &= \gamma_i^p\gamma_1^{-p}\end{aligned}$$

并根据引理 10.29 知此群等于 $(1+\gamma'+\cdots+(\gamma')^{p-1})Y$. 按上面这样, 引理 10.28 便得到了证明, 从而定理 10.25 也就得证. ∎

如果将引理 10.28 的推理应用到 $n > N$ 的 n, 那么便得到了

$$\mathrm{Ker}(X \to A_{K_n}) = (1+\gamma'+\cdots+(\gamma')^{p^{n-N}-1})Y.$$

因此得到了下面的引理.

引理 10.30 对于 $n > N$, 由自然映射 $X \to A_{K_n}$ 推导出同构

$$X/(1+\gamma'+\cdots+(\gamma')^{p^{n-N}-1})Y \xrightarrow{\sim} A_{K_n}. \qquad \square$$

像在 §10.0(c) 所谈及的那样, 关于 A_{K_n} 的阶, 岩泽证明了下面漂亮的公式 (称之为**岩泽公式**). 可将其叙述为: 令 $\lambda = \lambda(X)$, $\mu = \mu(X)$, 并令

$$\# A_{K_n} = p^{e_n},$$

则存在 $\nu \in \mathbb{Z}$, 使得对于所有充分大的 n 成立

$$e_n = \lambda n + \mu p^n + \nu.$$

使用引理 10.30, 那么这个公式可由考察当 n 充分大时的 $\#Y/(1+\gamma'+\cdots+(\gamma')^{p^n-1})Y$ 而得到.

在此, 或许是由于 $\mu = 0$ 常常成立的缘故吧, 称这个猜想为岩泽的 $\mu = 0$ 猜想. 如果 $K/\mathbb{Q}$ 为 Abel 扩域, Ferrero–Washington 给出了它的证明 (参看 §10.3(d)). 另外, 对于不是分圆 $\mathbb{Z}_p$ 扩域的 $\mathbb{Z}_p$ 扩张 (Galois 群为 $\mathbb{Z}_p$ 的扩张), 上面的公式也成立. 这时, 有使得 $\mu > 0$ 成立的扩域的例子 (岩泽).

问题 5 证明, 当 Y 作为 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K_N)]]$ 模同构于 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K_N)]]/(\gamma'-1-p)$ 时, 或者同构于 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K_N)]]/((\gamma'-1)^2-p)$ 时, 上面的岩泽公式成立.

作为引理 10.30 的又一个应用, 我们来证明, 当 K 具有某种特殊性质时, 由 X 的信息能够直接得到 A_{K_n} 的信息.

命题 10.31 假定 p 之上的 K 的素理想是唯一的, 并且它的素理想在 K_∞/K 中为完全分歧. 设 γ 是 $\Gamma = \mathrm{Gal}(K_\infty/K)$ 作为 $\mathbb{Z}_p$ 模的生成元, 且记满足 $\mu_{p^n} \subset K$ 的最大的 n 为 N (因此有 $K = K_N$). 此时, 对于任意的 $n \geqslant 0$, 关于 $K_{N+n} = K(\mu_{p^{n+N}})$ 成立同构

$$X/(\gamma^{p^n} - 1)X \xrightarrow{\sim} A_{K_{N+n}}. \qquad \square$$

例如, 如果 $K = \mathbb{Q}(\mu_{2p})$ 则满足此假定. 关于在 §10.0(c) 中作为例子叙述的三个二次域 K 中, $K(\mu_3)$ 对于 $p = 3$, 也满足这个条件.

[证明] 按照假定, 定理 10.25 的证明中的 r 可理解为 $r = 1$ (r 为 p 之上的 K_N 的素理想的个数). 因此 $\gamma' = \gamma$, 按照定理 10.29 有 $Y = (\gamma - 1)X$. 于是由引理 10.30 得出结论. ∎

(g) Abel 域的理想类群的负号部分

在此 (g) 小节中, 假设 p 为奇素数. 这里的 $K/\mathbb{Q}$ 为有限 Abel 扩域, 并也与 (e) 小节一样, 假设有 $\mu_p \subset K$. 当 X 如 (e) 中同样定义时, 复共轭 ρ 作用在 X 上, 我们在此小节的目标是要证明 $X^- = \{x \in X \mid \rho(x) = -x\}$ 是一个有限生成自由 $\mathbb{Z}_p$ 模.

一般地对于复共轭 ρ 作用于 $\mathbb{Z}_p$ 模 M, 我们令

$$M^+ = \{x \in M \mid \rho(x) = x\}$$
$$M^- = \{x \in M \mid \rho(x) = -x\}.$$

由假定 $p \neq 2$, 根据命题 10.12 因此有

$$M = M^+ \oplus M^-.$$

(也可写为 $M^+ = \dfrac{1+\rho}{2}M$, $M^- = \dfrac{1-\rho}{2}M$.)

设 K 如上, 像 (e) 中那样对 $n \geqslant 1$ 令 $K_n = K(\mu_{p^n})$. 因为 $\mathrm{Gal}(K_n/\mathbb{Q})$ 中的复共轭 ρ 作用于理想类群 $Cl(K_n)$ 上, 故而也作用于 p-Sylow 群 A_{K_n}. 于是有分解

$$A_{K_n} = A_{K_n}^+ \oplus A_{K_n}^-.$$

另外, 由于 $\mathrm{Gal}(K_\infty/\mathbb{Q})$ 中的复共轭也作用于 $X = \varprojlim A_{K_n}$, 故有分解

$$X = X^+ \oplus X^-,$$

并且 $X^+ = \varprojlim A_{K_n}^+$, $X^- = \varprojlim A_{K_n}^-$; 当令 $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$ 时, 这两个都是 Λ 模.

应用 Ferrero–Washington 定理 (定理 10.9), 则可证明 $\mu(X^-) = 0$ (见 §10.3(d)). 使用这个结果我们便能得到下面的定理.

定理 10.32 (岩泽, Ferrero–Washington) 作为 $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$ 模的 X^- 在 (b) 小节的意义下是 $\mathbb{Z}_p$ 自由的, 就是说, X^- 为有限生成自由 $\mathbb{Z}_p$ 模. $\square$

与其相反, 一般地 X^+ 并不是自由 $\mathbb{Z}_p$ 模. 譬如, 用在 §10.0(c) 中所说的例子, 可以证明当 $K = \mathbb{Q}(\sqrt{-762}, \sqrt{-3})$, $p = 3$ 时,

$$X^- \simeq \mathbb{Z}_3$$
$$X^+ \simeq \mathbb{Z}/243.$$

在证明定理 10.32 之前我们先证明下面的命题.

命题 10.33 对于 $m > n$, $A^-_{K_n} \to A^-_{K_m}$ 为单射.

[证明] 设 $K_{n+1} \neq K_n$, 只要能证明 $A^-_{K_n} \to A^-_{K_{n+1}}$ 为单射就足够了. 设 $\boldsymbol{a}$ 为 K_n 的理想且其类 $[\boldsymbol{a}]$ 属于 $A^-_{K_n}$, 并且它在 $A^-_{K_n} \to A^-_{K_{n+1}}$ 下的像为 0. 下面我们来证明 $[\boldsymbol{a}] = 0$.

因为 $[\boldsymbol{a}O_{K_{n+1}}] = 0$, 故可写为 $\boldsymbol{a}O_{K_{n+1}} = (x)$, $x \in K_{n+1}$. 设 $\mathrm{Gal}\,(K_{n+1}/K_n)$ 的生成元为 σ. 由于 $\sigma(\boldsymbol{a}O_{k_{n+1}}) = \boldsymbol{a}O_{k_{n+1}}$, 故有 $(\sigma(x)/x) = (1)$, 记

$$\frac{\sigma(x)}{x} = e, \quad e \in O^\times_{K_{n+1}}.$$

另一方面, 设 ρ 为复共轭并令

$$y = \frac{\rho(x)}{x},$$

由于 $\mathrm{Gal}\,(K_{n+1}/\mathbb{Q})$ 为 Abel 群故 σ 与 ρ 可交换, 从而

$$\frac{\sigma(y)}{y} = \frac{\rho(e)}{e} \in O^\times_{K_{n+1}}.$$

设 v 为 K_{n+1} 的任意的无限素点, $|\,|_v$ 为对应的绝对值, 于是 $|\sigma(y)/y|_v = |\rho(e)/e|_v = |e|_v/|e|_v = 1$, 从而有 $\log|\sigma(y)/y|_v = 0$. 因为 K_{n+1} 的导子非 0 (参照 §7.5), 这意味着 $\sigma(y)/y$ 为单位根, 于是存在与 p 互素的整数 c 使得

$$\left(\frac{\sigma(y)}{y}\right)^c \in \mu_{p^{n+1}}.$$

设 $N_{K_{n+1}/K_n} : K^\times_{n+1} \to K^\times_n$ 为范映射, 那么由于 $N_{K_{n+1}/K_n}(\sigma(y)/y) = 1$, 由下面的引理 10.34(1) 有

$$\left(\frac{\sigma(y)}{y}\right)^c \in \mu_p.$$

另外, 按照引理 10.34(2), 存在 ζ 使得

$$\left(\frac{\sigma(y)}{y}\right)^c = \frac{\sigma(\zeta)}{\zeta}, \ \zeta \in \mu_{p^{n+1}}.$$

令

$$z = \frac{y^c}{\zeta},$$

由于 $\sigma(z)=z$, 故按照 Galois 理论有 $z\in K_n$ 使得

$$zO_{K_{n+1}}=y^cO_{K_{n+1}}=\frac{\rho(\boldsymbol{a}^cO_{K_{n+1}})}{\boldsymbol{a}^cO_{K_{n+1}}}.$$

所以作为 K_n 的理想有

$$zO_{K_n}=\frac{\rho(\boldsymbol{a}^c)}{\boldsymbol{a}^c}.$$

如果在 $Cl(K_n)$ 中考察, 它便是

$$0=[(z)]=-2c[\boldsymbol{a}],$$

因为 $2c$ 与 p 互素, 故得到 $[\boldsymbol{a}]=0$. ∎

引理 10.34

(1) 如果 $\zeta\in\mu_{p^{n+1}}$, $N_{K_{n+1}/K_n}(\zeta)=1$, 则 $\zeta\in\mu_p$.

(2) 如果 $\zeta\in\mu_p$, 则有 $\zeta'\in\mu_{p^{n+1}}$ 使得 $\sigma(\zeta')/\zeta'=\zeta$.

[证明] (1) 设 $\zeta_{p^{n+1}}$ 为 p^{n+1} 次本原单位根, 对于任意 $a\in\mathbb{Z}$, 由于有 $N_{K_{n+1}/K_n}(\zeta_{p^{n+1}}^a)=\zeta_{p^{n+1}}^{ap}$, 故而立即得到所要的.

(2) 因为 $\zeta_{p^{n+1}}\notin K_n$, 故 $\sigma(\zeta_{p^{n+1}})/\zeta_{p^{n+1}}$ 为 p 次本原单位根. 因此得到 (2). ∎

注记 命题 10.33 的证明是没有使用下列的上同调

$$\mathrm{Ker}(A_{K_n}^-\to A_{K_{n+1}}^-)\hookrightarrow H^1(K_{n+1}/K_n,O_{K_{n+1}}^\times)^-=H^1(K_{n+1}/K_n,\mu_{p^{n+1}})=0$$

而得到的结果.

[定理 10.32 的证明] 按照命题 10.22, 只要能证明 X^- 不具有 0 以外的有限 Λ 子模, 并且 $\mu(X^-)=0$ 就可以了. 我们将在 §10.3(d) 看到 $\mu(X^-)=0$ 的证明, 而在这里我们来证明前者. 假设 $x\in X^-$ 生成的 X^- 的 Λ 子模 M 为有限. 又设 γ 为 $\Gamma=\mathrm{Gal}(K_\infty/K)$ 作为 $\mathbb{Z}_p$ 模的生成元, 那么由于 $\gamma^{p^n}\to 1\ (n\to\infty)$, 故有

$$\lim_{n\to\infty}\gamma^{p^n}(x)=x.$$

由 M 是有限的假定知 M 是离散的, 对于充分大的 $c>0$ 有 $\gamma^{p^c}(x)=x$.

取 n_0 为使得作为 $\mathbb{Z}_p$ 模的 $\mathrm{Gal}(K_\infty/K_{n_0})$ 由 γ^{p^c} 生成的最大的 n_0. 对于满足 $n\geqslant n_0$ 的 n, 设

$$\varphi_n: X^-\to A_{K_n}^-$$

为自然映射, 我们来证明 $\varphi_n(x)=0$. 如果能证明它, 那么就有 $x=0$, 从而 $M=0$, 于是就证明了 X^- 不具有 0 以外的有限 Λ 子模.

设 M 的阶为 p^m. 考虑范映射 $N: A_{K_{n+m}}^-\to A_{K_n}^-$ 与自然映射 $i: A_{K_n}^-\to A_{K_{n+m}}^-$, 则有

$$i\circ N=\sum_{\sigma\in\mathrm{Gal}(K_{n+m}/K_n)}\sigma.$$

因为由假定, $\mathrm{Gal}\,(K_\infty/K_{n_0})$ 对 x 的作用是平凡的, 故 $\sigma \in \mathrm{Gal}\,(K_{n+m}/K_n)$ 对 $\varphi_{n+m}(x)$ 的作用也是平凡的. 因此有

$$\begin{aligned} i \circ N \circ \varphi_{n+m}(x) = p^m \varphi_{n+m}(x) &= \varphi_{n+m}(p^m x) \\ &= \varphi_{n+m}(0) = 0. \end{aligned}$$

另一方面, 因为 $N \circ \varphi_{n+m}(x) = \varphi_n(x)$ 故得到了

$$i(\varphi_n(x)) = 0,$$

由命题 10.33 知 i 为单射, 故而有 $\varphi_n(x) = 0$. ∎

§10.3 岩泽主猜想

在此使用 §10.1, §10.2 的结果, 终于可以叙述岩泽主猜想了. §10.1 中所叙述的存在于 p 进世界中的 p 进 L 函数, 在此直接地与 §10.2 所叙述的分圆 $\mathbb{Z}_p$ 扩域的理想类群联系起来. 在此 §10.3 中我们也将叙述岩泽主猜想的应用及证明的思路, 以及相关的话题.

(a) 岩泽主猜想的阐述

设 p 为素数, N 为正整数,

$$\chi : (\mathbb{Z}/N)^\times \to \overline{\mathbb{Q}}_p^\times$$

为取值于 $\overline{\mathbb{Q}}_p^\times$ 中的本原 Dirichlet 特征. 进一步用 §10.1(e) 的话说就是, χ 是第一类 Dirichlet 特征. 我们写成

$$N = N_0 p^a, \quad N_0 与\ p\ 互素.$$

根据第一类 Dirichlet 特征的定义, 当 p 为奇素数时 $a = 0$ 或 $a = 1$, 而当 $p = 2$ 时则 $a = 0$ 或 $a = 2$.

与迄今为止一样, 设 μ_n 为 $\overline{\mathbb{Q}}$ 中的 n 次单位根全体构成的群, 令

$$\begin{aligned} K_n &= \mathbb{Q}(\mu_{N_0 p^n}) \\ K_\infty &= \mathbb{Q}(\mu_{N_0 p^\infty}) = \bigcup_{n \geqslant 1} K_n. \end{aligned}$$

又令

$$K = \begin{cases} K_1 & 当\ p\ 为奇素数 \\ K_2 & p = 2. \end{cases}$$

像在 §10.1(e) 中那样, 令

$$\Delta = \mathrm{Gal}\,(K/\mathbb{Q})$$
$$\Gamma = \mathrm{Gal}\,(K_\infty/K),$$

则有

$$\mathrm{Gal}\,(K_\infty/\mathbb{Q}) = \Delta \times \Gamma.$$

由 $N = N_0p^a$ 及 K 的定义, 并因为有自然映射

$$\Delta = \mathrm{Gal}\,(K/\mathbb{Q}) \to (\mathbb{Z}/N)^\times,$$

那么由此映射与 χ 的复合, 可将 χ 看成是 Δ 的特征.

下面像 §10.1 那样考虑完备群环. 设 $O_\chi = \mathbb{Z}_p[\mathrm{Image}\,\chi]$ 为由 χ 的像在 $\mathbb{Z}_p$ 上生成的环. 令

$$\Lambda_{N_0} := \mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/\mathbb{Q})]] = \mathbb{Z}_p[[\Delta \times \Gamma]]$$
$$\Lambda_\chi := O_\chi[[\mathrm{Gal}\,(K_\infty/K)]] = O_\chi[[\Gamma]].$$

像在 §10.1(e) 中一样定义同态映射

$$\phi_\chi : \Lambda_{N_0} = \mathbb{Z}_p[[\Delta \times \Gamma]] \to \Lambda_\chi = O_\chi[[\Gamma]]$$

为满足

$$\phi_\chi \left(\sum_{(\sigma,\tau)\in\Delta\times\Gamma} a_{\sigma\tau}(\sigma,\tau) \right) = \sum a_{\sigma\tau}\chi(\sigma)\tau$$

的映射. 依照 ϕ_χ 可将 Λ_χ 看作 Λ_{N_0} 模.

下面设 A_{K_n} 为 K_n 的理想类群的 p-Sylow 群 (p 部分), 与 §10.2(e) 一样, 考虑按照范映射取逆极限

$$X_{K_\infty} = \varprojlim A_{K_n}.$$

根据定理 §10.25, X_{K_∞} 为有限生成扭 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K)]]$ 模. 另外从 $\mathrm{Gal}\,(K_\infty/\mathbb{Q})$ 作用于 X_{K_∞} 上, 知 X_{K_∞} 也为 Λ_{N_0} 模. 因为 $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \subset \Lambda_{N_0}$, 故 X_{K_∞} 为有限生成扭 Λ_{N_0} 模. 现在我们定义 X_{K_∞} 的 χ 分量为

$$(X)_\chi = X_{K_\infty} \otimes_{\Lambda_{N_0}} \Lambda_\chi.$$

由上所述, $(X)_\chi$ 成为了有限生成扭 Λ_χ 模 (请注意, 按照 ϕ_χ 将 Λ_χ 看作 Λ_{N_0} 模, 而 $\Lambda_{N_0} \otimes_{\Lambda_{N_0}} \Lambda_\chi = \Lambda_\chi$). 固定 Γ 作为 $\mathbb{Z}_p$ 模的一个生成元 γ, 由此, 我们注意到, 由命题 10.10 得到了同构

$$\Lambda_\chi = O_\chi[[\Gamma]] \simeq O_\chi[[T]]$$
$$\gamma \leftrightarrow 1 + T.$$

于是, 根据定义 10.21,

$$\mathrm{Char}\,((X)_\chi) \subset \Lambda_\chi \simeq O_\chi[[T]]$$

定义了 Λ_χ 的一个主理想. $\mathrm{Char}\,((X)_\chi)$ 是包含了理想类群和 Galois 群作用的信息的 Λ_χ 的理想.

设 ω 为 Teichmüller 特征, 试着考虑当 $\chi = \omega$ 的情形, 可以证明 $(X)_\omega = 0$ (参看下面 (b) 小节). 那么, 下面便设 $\chi \neq \omega$. 于是, $\chi^{-1}\omega \neq \mathbf{1}$. 由于定理 10.7 的缘故, 存在幂级数 $G_{\chi^{-1}\omega}(T) \in O_\chi[[T]]$ 使得

$$G_{\chi^{-1}\omega}(u^s - 1) = L_p(s, \chi^{-1}\omega),\ u = \kappa(\gamma).$$

这里的 κ 为分圆特征, γ 为 Γ 的一个固定了的生成元. 这时, 所谓的岩泽主猜想便是下面的定理.

定理 10.35 (岩泽主猜想) 设 χ 为奇特征 $(\chi(-1) = -1)$ 并为满足 $\chi \neq \omega$ 的第一类特征. 于是, 若将 $(X)_\chi$ 的特征理想 $\mathrm{Char}\,((X)_\chi)$ 看作是 $\Lambda_\chi \simeq O_\chi[[T]]$ 中的理想时, 则成立

$$\mathrm{Char}\,((X)_\chi) = \left(\frac{1}{2}G_{\chi^{-1}\omega}(T)\right). \qquad \square$$

在上面的等式中, 左端是由理想类群决定的代数的、数论的对象, 而右端则是由 ζ 函数、L 函数的值所决定的 p 进解析的对象. 在数论的许多漂亮的定理之中, 这个定理是特别值得玩味的、优美的定理之一. 这个定理, 当 p 为奇素数时已由 Mazur 和 Wiles(1985年) 证明, 对于 $p = 2$ 的情形 (及对于全实数域上的特征) 由 Wiles(1990年) 证明, 他们的证明都实质性地使用了自守形式.

在此之后, Rubin 完成了 Kolyvagin 的设想, 对于几乎所有的 χ 仅用代数数论方法给出了证明 (1990年). 在这个证明中, 使用了 Kolyvagin 所发现的称作 Euler 系的概念. 另外, Greither 还确认了在包含 $p = 2$ 的一般情形时使用 Euler 系进行证明是可行的 (1992年).

(b) $\mathbb{Q}(\mu_{p^\infty})$ 的理想类群

在本小节 (b) 中我们将通过对 $\mathbb{Q}(\mu_{p^\infty})$ 情形的详尽讨论来认识岩泽主猜想. 也就是说, 讨论在 (a) 的记号中 $N_0 = 1$ 的情形. 下面我们记

$$X = X_{\mathbb{Q}(\mu_{p^\infty})} = \varprojlim A_{\mathbb{Q}(\mu_{p^n})}.$$

首先根据命题 10.31, 设 γ 为 $\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_{2p}))$ 的生成元, 从而成立

$$X/(\gamma - 1)X \xrightarrow{\sim} A_{\mathbb{Q}(\mu_{2p})}.$$

于是, 由中山引理知 $X \neq 0$ 与 $A_{\mathbb{Q}(\mu_{2p})} \neq 0$ 等价. 总之, 使得 $X \neq 0$ 仅限于 p 为非正则素数时 (参照 §10.0(a)). 特别地, 由于 $p = 2$ 时 $X = 0$, 那么以下我们总设 p 为奇素数.

由于 $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ 的 Galois 群有分解

$$\begin{aligned}\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) &= \Delta \times \Gamma \\ \Delta &= \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \\ \Gamma &= \mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)),\end{aligned}$$

可以将 $\Lambda_1 = \mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]] = \mathbb{Z}_p[\Delta][[\Gamma]]$ 模 X 看作 $\mathbb{Z}_p[\Delta]$ 模. Δ 的阶为 $p-1$, 又设 ω 为 Δ 的 Teichmüller 特征, 将 Δ 的任意特征写成

$$\omega^i\,(i = 0, 1, \cdots, p-2)$$

的形式. 于是, 如果我们注意到 $\mathbb{Z}_p$ 包含了所有 $p-1$ 次单位根的话, 那么就可以应用命题 10.12 得到分解

$$\begin{aligned}X &= \bigoplus_{i=0}^{p-2} X^{\omega^i} \\ X^{\omega^i} &= \{x \in X \mid \text{对于所有的 } \sigma \in \Delta \text{ 有 } \sigma(x) = \omega^i(\sigma)x\}.\end{aligned}$$

每个 X^{ω^i} 是 $\mathbb{Z}_p[[\Gamma]]$ 模.

这也看成是对各有限次数域的理想类群的 ω^i 部分的逆极限. 也就是说, 令

$$K_n = \mathbb{Q}(\mu_{p^n}).$$

由 $\mathrm{Gal}\,(K_n/\mathbb{Q}) = \Delta \times \mathrm{Gal}\,(K_n/\mathbb{Q}(\mu_p))$ 知, Δ 作用于 A_{K_n}. 因此由命题 10.12 有分解

$$\begin{aligned}A_{K_n} &= \bigoplus_{i=0}^{p-2} A_{K_n}^{\omega^i} \\ A_{K_n}^{\omega^i} &= \{x \in A_{K_n} \mid \text{对所有 } \sigma \in \Delta, \text{有} \sigma(x) = \omega^i(\sigma)x\}.\end{aligned}$$

于是有

$$X^{\omega^i} = \varprojlim A_{K_n}^{\omega^i}.$$

对于 X^{ω^i} 成立下面的定理.

定理 10.36 令 $X = X_{\mathbb{Q}(\mu_{p^\infty})} = \varprojlim A_{\mathbb{Q}(\mu_{p^n})}$. 对于奇素数 p 有分解

$$X = \bigoplus_{i=0}^{p-2} X^{\omega^i}.$$

(1) 设 γ 为 $\Gamma = \mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p))$ 的 (拓扑) 生成元, 并令 $K_n = \mathbb{Q}(\mu_{p^\infty})$, 则自然映射 $X^{\omega^i} \to A_{K_n}^{\omega^i}$ 诱导出同构

$$X^{\omega^i}/(\gamma^{p^n-1} - 1)X^{\omega^i} \xrightarrow{\sim} A_{K_n}^{\omega^i}.$$

(2) 当 i 为奇数时, X^{ω^i} 为有限生成的自由 $\mathbb{Z}_p$ 模.

(3) 对于奇数 i, 设 λ_i 为 X^{ω^i} 的 $\mathbb{Z}_p$ 秩, 即

$$X^{\omega^i} \simeq \mathbb{Z}_p^{\lambda_i}.$$

于是, $\gamma - 1$ 倍映射

$$X^{\omega^i} \to X^{\omega^i}$$

$$x \mapsto (\gamma - 1)x$$

是 $\mathbb{Z}_p$ 线性映射的, 从而可用矩阵 $V_{\gamma-1} \in M_{\lambda_i}(\mathbb{Z}_p)$ 来表示. 作为 $\mathbb{Z}_p[[T]]$ 模的 X^{ω^i} 的特征理想 $\mathrm{Char}\,(X^{\omega^i})$ 在同构

$$\mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]]$$

$$\gamma \leftrightarrow 1 + T$$

之下可看成为 $\mathbb{Z}_p[[T]]$ 的理想, 于是 $\mathrm{Char}\,(X^{\omega^i})$ 由 $V_{\gamma-1}$ 的特征多项式生成. 也就是说有

$$\mathrm{Char}\,(X^{\omega^i}) = (\det(TI - V_{\gamma-1})).$$

[证明] (1) 由命题 10.31 有

$$X/(\gamma^{p^{n-1}} - 1)X = A_{K_n}.$$

取其各个 ω^i 分量, 就得到了 (1).

(2) 设 X^- 如同 §10.2(g) 中那样, 那么由定义便有

$$X^- = \bigoplus_{\substack{i=1 \\ i:\text{奇数}}}^{p-2} X^{\omega^i}.$$

由定理 10.32 知 X^- 为有限生成自由 $\mathbb{Z}_p$ 模, 故而每个 X^{ω^i} 也为有限生成自由 $\mathbb{Z}_p$ 模.

(3) 因为 X^{ω^i} 为 $\mathbb{Z}_p$ 自由的有限生成扭 $\mathbb{Z}_p[[\Gamma]]$ 模, 从而由命题 10.23(4) 得到结论. ∎

像 (a) 小节那样, 定义 $(X)_{\omega^i}$ 为 $(X)_{\omega^i} = X \otimes_{\Lambda_1} \Lambda_{\omega^i}$, 并有

$$X^{\omega^j} \otimes_{\Lambda_1} \Lambda_{\omega^i} = \begin{cases} X^{\omega^i} & \omega^i = \omega^j \\ 0 & \omega^i \neq \omega^j. \end{cases}$$

因此有

$$(X)_{\omega^i} = X^{\omega^i}.$$

由此, 并根据定理 10.36(3)(以及关于 $\varinjlim$ 和 $\varprojlim$ 的考察), 便知道在 §10.0(e) 所叙述的岩泽主猜想与在定理 10.35 中所叙述的岩泽主猜想是一致的.

另外我们还注意到, 由 $A^{\omega}_{\mathbb{Q}(\mu_p)}=0$ (这个断言, 譬如, 可利用将在 (d) 小节中叙述的 Stickelberger 定理得知), 并根据定理 10.36(1) 与中山引理, 可得到 $X^{\omega}=0$.

正如在定理 10.36(2) 中见到的那样, 对于奇数 i, X^{ω^i} 为自由 $\mathbb{Z}_p$ 模. 那么它的秩具体地是多少呢? 按照对于 $p<12,000,000$ 范围内的计算有

$$X^{\omega^i}\simeq\mathbb{Z}_p \text{ 或者 } 0.$$

若设 X^{ω^i} 的秩为 λ_i, 那么就是 $\lambda_i=1$ 或者 0. 在计算 λ_i 时, 若使用岩泽主猜想 (定理 10.35) 有

$$\lambda_i=\lambda(G_{\omega^{1-i}}(T)),$$

故而只要计算 $G_{\omega^{1-i}}(T)$ 就可以了. 根据将在 (d) 小节所讲, $G_{\omega^{1-i}}(T)$ 是能够具体计算的.

问题 6 使用岩泽主猜想证明以下断言.

(1) 设 i 为满足 $1<i<p-2$ 的奇数. 证明, 如果有

$$\zeta(1+i-p)\not\equiv\zeta(2+i-2p)\pmod{p^2},$$

则有 $\lambda(G_{\omega^{1-i}}(T))\leqslant 1$. 因此, $X^{\omega^i}\simeq\mathbb{Z}_p$ 或者 0.(提示: 使用问题 4(§10.1(c)).)

(2) 对于 $p=37, i=5$, 确认 (1) 中的关系成立.

(3) 对于 $p=691$, $i=697, 491$, 想出高效率的计算 $\zeta(1-r)\bmod p^2$ (r: 正整数) 值的方法, 并由此确认 (1) 的关系成立.

下面讲述当 i 为偶数时, X^{ω^i} 又是怎样的情况. 首先, 立即可知有 $X^{\omega^0}=0$. 于是设 i 为满足 $0<i<p-1$ 的偶数. 根据对 $p<12,000,000$ 范围的计算有

$$X^{\omega^i}=0.$$

于是有所谓的 **Vandiver 猜想**说, 对于任意的 p 以及任意的偶数 i 成立 $X^{\omega^i}=0$. 稍许弱一点有所谓 **Greenberg 猜想**, 说 X^{ω^i} 为有限.

Greenberg 猜想表达的是更一般的陈述, 即对于任意的偶特征 χ, $(X)_\chi$ 为有限 (推广到任意数域). 也就是说, 对于偶特征 χ, 成立 $\operatorname{Char}((X)_\chi)=\Lambda_\chi$. 然而除了知道关于 Vandiver 猜想以及 Greenberg 猜想的许多实例 (还不知有反例) 外, 却并没有找到根据.

关于 Vandiver 猜想, 仅能证明对于任意的 p 有

$$X^{\omega^{p-3}}=0$$

成立. 其证明实质性地使用 K 理论. 对于其他的偶数 i $(0<i<p-1)$, 还不知道有

这样的一般性结果.

(c) 理想类群的 χ 分量的阶与 ζ 函数值的意义

设 p 为奇素数并按照 (b) 小节那样, 分解

$$A_{\mathbb{Q}(\mu_p)} = \bigoplus_{i=0}^{p-2} A_{\mathbb{Q}(\mu_p)}^{\omega^i}.$$

应用岩泽主猜想, 完全可以用 L 函数的值表达出 $A_{\mathbb{Q}(\mu_p)}^{\omega^i}$ 的阶.

定理 10.37 对于满足 $1 < i < p-1$ 的奇数 i, 成立

$$\# A_{\mathbb{Q}(\mu_p)}^{\omega^i} = \#(\mathbb{Z}_p / L(0, \omega^{-i})).$$

这里, $L(s, \omega^{-i})$ 为 Dirichlet L 函数.

[证明] 与 (b) 相同, 令 $X = X_{\mathbb{Q}(\mu_{p^\infty})}$. 又令 $\Lambda = \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]]$. 将 X^{ω^i} 看作 Λ 模, 那么应用命题 10.20 则可写

$$X^{\omega^i} \sim \Lambda/(f_1^{n_1}) \oplus \cdots \oplus \Lambda/(f_r^{n_r}).$$

由伪同构的定义知存在正合序列

$$0 \to (\text{有限}) \to X^{\omega^i} \xrightarrow{\Phi} \Lambda/(f_1^{n_1}) \oplus \cdots \oplus \Lambda/(f_r^{n_r}) \to (\text{有限}) \to 0.$$

设 γ 为 Γ 的生成元, 根据定理 10.36(1) 有 $X^{\omega^i}/(\gamma - 1)X^{\omega^i} \xrightarrow{\sim} A_{\mathbb{Q}(\mu_p)}^{\omega^i}$, 又由定理 10.36(2) 知 Φ 为单射.

因此, 存在以下的正合序列的交换图表.

$$\begin{array}{ccccccc}
 & & & & & & 0 \\
 & & & & & & \downarrow \\
 & & & & 0 & & \operatorname{Ker} T_c \\
 & & & & \downarrow & & \downarrow \\
0 \to & X^{\omega^i} & \xrightarrow{\Phi} & & \Lambda/(f_1^{n_1}) \oplus \cdots \oplus \Lambda/(f_r^{n_r}) & \to & \operatorname{Coker} \Phi \to 0 \\
 & \downarrow{\scriptstyle \gamma - 1} & & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T_c} \\
0 \to & X^{\omega^i} & \xrightarrow{\Phi} & & \Lambda/(f_1^{n_1}) \oplus \cdots \oplus \Lambda/(f_r^{n_r}) & \to & \operatorname{Coker} \Phi \to 0 \\
 & \downarrow & & & \downarrow & & \downarrow \\
 & A_{\mathbb{Q}(\mu_p)}^{\omega^i} & \to & & \mathbb{Z}_p/(f_1(0)^{n_1}) \oplus \cdots \oplus \mathbb{Z}_p/(f_r(0)^{n_r}) & \to & \operatorname{Coker} T_c \to 0 \\
 & \downarrow & & & \downarrow & & \downarrow \\
 & 0 & & & 0 & & 0
\end{array}$$

这里, 正中的列映射分别为 $\gamma - 1$ 倍的, T 倍的, 以及 T 倍在 $\operatorname{Coker}\Phi$ 上的诱导的映射. 由于 $\operatorname{Coker}\Phi$ 为有限故由图表知 $\operatorname{Ker}T_c$ 与 $\operatorname{Coker}T_c$ 的阶相等. 因此由蛇形引理

得到

$$\#A_{\mathbb{Q}(\mu_p)}^{\omega^i} = \#(\mathbb{Z}_p/(f_1(0)^{n_1}) \oplus \cdots \oplus \mathbb{Z}_p/(f_r(0)^{n_r})).$$

再由岩泽主猜想 (定理 10.35) 有

$$\mathrm{Char}\,(X^{\omega^i}) = (f_1^{n_1} \cdots f_r^{n_r}) = (G_{\omega^{1-i}}(T)),$$

故而有

$$\#A_{\mathbb{Q}(\mu_p)}^{\omega^i} = \#(\mathbb{Z}_p/(G_{\omega^{1-i}}(0))).$$

根据定理 10.7, 定理 10.6, 由于有

$$G_{\omega^{1-i}}(0) = L_p(0, \omega^{1-i}) = L(0, \omega^{-i}),$$

故而得到了定理 10.37 的结论. ∎

更一般地, 对于奇特征 χ, 设 K 为 χ 的核所对应的域, 即使得 $\mathrm{Gal}\,(K/\mathbb{Q}) \simeq \mathrm{Im}\,\chi$ 成立的域, 又设 $O_\chi = \mathbb{Z}_p[\mathrm{Im}\,\chi]$, 那么我们已能够知道

$$(A_K \otimes O_\chi)^\chi = \{x \in A_K \otimes O_\chi \mid \text{对所有 } \sigma \in \mathrm{Gal}\,(K/\mathbb{Q}) \text{ 有 } \sigma(x) = \chi(\sigma)x\}$$

的阶可以用 $L(0, \chi^{-1})$ 来表示 (Mazur, Wiles, Solomon, Greither).

可以得到作为定理 10.37 的推论的以下 Herbrand, Ribet 的定理 (直接可以看出, 它等价于在 §10.0(b) 中叙述的 Herbrand, Ribet 定理.)

推论 10.38 (Herbrand, Ribet)　对于满足 $1 < i < p-1$ 的奇数 i, 下面的断言等价:

(1) $A_{\mathbb{Q}(\mu_p)}^{\omega^i} \neq 0$

(2) 对于满足 $i \equiv 1 - r \pmod{p-1}$ 的正整数 $r > 0$, $\zeta(1-r)$ 的分子被 p 除尽.

[证明]　这是由于我们知道有

$$\begin{aligned} L(0, \omega^{-i}) &= L_p(0, \omega^{1-i}) = L_p(0, \omega^r) \\ &\equiv \zeta(1-r) \pmod{p}. \end{aligned}$$

最后的那个同余式来自定理 10.6 及命题 10.8. ∎

那么, $\zeta(1-r)$ 自身又具有什么样的意义呢? 当我们把它写成既约分数的形式

$$\zeta(1-r) = \pm \frac{N_r}{D_r}$$

时, 对于 N_r 与 D_r 的意义, 当应用岩泽主猜想时便知道有如下的事实 (将不予证明): 令

$$\mathbb{Z}_p(1) = \varprojlim \mu_{p^n} \quad (\text{关于 } p \text{ 幂映射的逆极限})$$

$$\mathbb{Z}_p(m) = \underbrace{\mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \cdots \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)}_{m\text{个}}.$$

$\mathbb{Z}_p(m)$ 作为 $\mathbb{Z}_p$ 模是秩为 1 的自由模, 而 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 以分圆特征 κ 的 m 次幂作用于它. (即若设 $x \in \mathbb{Z}_p(m)$, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, 则 $\sigma(x) = \kappa(\sigma)^m x$.)

对于有 Galois 群作用的任意 $\mathbb{Z}_p$ 模 M 而言, 我们定义 $M(m)$ 为

$$M(m) = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(m),$$

并称其为 M 的 **Tate 扭转** (Tate twist). 此时, 对于任意的偶数 $r > 0$, 可以证明

$$X_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^{1-r}}(r-1)/(\gamma-1)X_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^{1-r}}(r-1)$$

为有限, 并能证明

$$N_r = \prod_p \#(X_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^{1-r}}(r-1)/(\gamma-1)X_{\mathbb{Q}(\mu_{p^\infty})}^{\omega^{1-r}}(r-1)).$$

这里的 p 遍历所有的素数 (实质上遍历所有的非正则素数). 对于分母, 可证明有

$$D_r = \prod_p \#(\mathbb{Q}_p/\mathbb{Z}_p(r))^{\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})}.$$

这里的 p 遍历所有的素数. $(\ )^{\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})}$ 表示 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$- 不变部分. 另外, $(r-1)$, (r) 为 Tate 扭转. 由此事实便推导出了命题 10.3(2). 也还有将 N_r, D_r 作为代数 K 群的阶的想法 (Quillen–Lichtenbaum 猜想).

问题 7 在承认 D_r 的上述表示下, 证明命题 10.3(2).

(d) Stickelberger 定理

设 N 为正整数. Stickelberger 受 Gauss, Kummer 等人研究的启发, 对于 $\mathbb{Q}(\mu_N)$ 的理想类群证明了下面将叙述的非常有名的定理 (1890年).

首先, 设

$$\zeta_{\equiv a(N)}(s) = \sum_{\substack{n=1 \\ n\equiv a \pmod N}}^{\infty} \frac{1}{n^s}$$

为部分 ζ 函数 (参看 §3.3 的定义 3.13). 按照同构 $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N)^\times$(参看 §5.2 的定理 5.4), 我们记 $a \in (\mathbb{Z}/N)^\times$ 所对应于这个 Galois 群中的元为 σ_a. 此时称

$$\theta_{\mathbb{Q}(\mu_N)} = \sum_{\substack{a=1 \\ (a,N)=1}}^{N} \zeta_{\equiv a(N)}(0)\sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})]$$

为 **Stickelberger 元** (Stickelberger element). 此处的和是对满足 $(a, N) = 1$ 的从 1 走到 N 的整数 a 取的.

更加具体地, 设 $0 < a < N$, 由于有

$$\zeta_{\equiv a(N)}(0) = -\frac{a}{N} + \frac{1}{2}$$

(§3.3(b) 的例 3.20), 故有

$$\theta_{\mathbb{Q}(\mu_N)} = \sum_{\substack{a=1 \\ (a,N)=1}}^{N} \left(-\frac{a}{N} + \frac{1}{2}\right)\sigma_a^{-1}.$$

在上面特意使用 ζ 函数来写出, 是为了能认识到 $\theta_{\mathbb{Q}(\mu_N)}$ 是处在 ζ 世界之中的.

Stickelberger 定理是说,

定理 10.39 (Stickelberger) 令

$$\theta'_{\mathbb{Q}(\mu_N)} = \theta_{\mathbb{Q}(\mu_N)} - \frac{1}{2} \sum_{\substack{a=1 \\ (a,N)=1}}^{N} \sigma_a.$$

设 $\alpha \in \mathbb{Z}[\mathrm{Gal}\,(\mathbb{Q}(\mu_N)/\mathbb{Q})]$ 满足

$$\alpha\theta'_{\mathbb{Q}(\mu_N)} \in \mathbb{Z}[\mathrm{Gal}\,(\mathbb{Q}(\mu_N)/\mathbb{Q})],$$

则对于理想类群 $Cl(\mathbb{Q}(\mu_N))$ 有

$$(\alpha\theta'_{\mathbb{Q}(\mu_N)})Cl(\mathbb{Q}(\mu_N)) = 0.$$ □

简而言之, 定理是说 Stickelberger 元零化理想类群. 这个定理的证明是根据对 Gauss 和的素理想分解的详细研究得到的. 我们在这里省略证明. 在此想要说的是岩泽所发现的 Stickelberger 元与 p 进 L 函数之间所具有的关系.

设 χ, K, K_n 同于 (a) 小节的那样. 有分解

$$\mathrm{Gal}\,(K_n/\mathbb{Q}) = \mathrm{Gal}\,(K/\mathbb{Q}) \times \mathrm{Gal}\,(K_n/K).$$

令 $O_\chi = \mathbb{Z}_p[\mathrm{Image}\,\chi]$, $\mathbb{Q}_p(\chi) = \mathbb{Q}_p(\mathrm{Image}\,\chi)$. 定义

$$\phi_{\chi,n} : \mathbb{Q}[\mathrm{Gal}\,(K_n/\mathbb{Q})] = \mathbb{Q}[\mathrm{Gal}\,(K/\mathbb{Q}) \times \mathrm{Gal}\,(K_n/K)] \to \mathbb{Q}_p(\chi)[\mathrm{Gal}\,(K_n/K)]$$

为

$$\phi_{\chi,n}(\sum a_{\sigma\tau}(\sigma,\tau)) = \sum a_{\sigma\tau}\chi(\sigma)\tau.$$

于是对于 $\chi \neq \omega$ 的奇特征 χ, 可以证明

$$\phi_{\chi,n}(\theta_{K_n}) \in O_\chi[\mathrm{Gal}\,(K_n/K)].$$

并且还能确定, $\phi_{\chi,n}(\theta_{K_n})$ 形成一个关于 n 的逆向系. 让 Λ_χ 同于 (a) 中所设, 令

$$\begin{aligned}\theta^{\chi}_{K_\infty} := (\phi_{\chi,n}(\theta_{K_n})) \in \varprojlim O_\chi[\mathrm{Gal}(K_n/K)] &= O_\chi[[\mathrm{Gal}(K_\infty/K)]] \\ &= \Lambda_\chi.\end{aligned}$$

固定 $\mathrm{Gal}\,(K_\infty/K)$ 的一个拓扑生成元 γ, 以此将 $\Lambda_\chi \simeq O_\chi[[T]]$ 看作一样.

定理 10.40 (岩泽) *设 χ 为满足 $\chi \neq \omega$ 的第一类奇特征, 则有*

$$\theta_{K_\infty}^{\chi} = G_{\chi^{-1}\omega}(T). \qquad \square$$

在此这一定理的证明仍被省略.

如在 §10.1(f) 曾谈及的, 使用这样的论断可以证明 p 进 L 函数的存在性. 由 Stickelberger 定理以及上面的定理 10.40 还可得出以下推论.

推论 10.41 *$G_{\chi^{-1}\omega}(T)$ 消去 $(X)_\chi$. 即*

$$G_{\chi^{-1}\omega}(T)(X)_\chi = 0. \qquad \square$$

这是因为由 Stickelberger 定理可证明 $\theta_{K_\infty}^{\chi}(X)_\chi = 0$ 的缘故. 感觉起来, 推论 10.41 非常接近于岩泽主猜想 (定理 10.35). 其实, 岩泽主猜想就是这样诞生的.

那么, 还是设 p 为奇素数吧. 由 Ferrero–Washington 定理 (定理 10.9) 有 $\mu(G_{\chi^{-1}\omega}(T)) = 0$ (μ 的定义在 §10.2(a)). 因此根据推论 10.41 得知 $\mu((X)_\chi) = 0$ (这个 μ 的定义在 §10.2(b)). 由此, 当把 $X_{K_\infty}^-$ 看作是 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K)]]$ 模时, 也就知道了

$$\mu(X_{K_\infty}^-) = 0.$$

以此便完成了对定理 10.32 (§10.2(g)) 的证明. 实际上更一般地, 对于任意的 p, 任意的 χ, 由定理 10.9 仍可证明 $\mu((X)_\chi) = 0$ 成立.

对于 λ 不变量, 岩泽利用类数公式证明了

$$\sum_{\chi} \lambda(G_{\chi^{-1}\omega}(T)) = \sum_{\chi} \lambda((X)\chi) \quad (\chi\text{遍历 } \mathrm{Gal}\,(K/\mathbb{Q})\text{的不等于 } \omega\text{的奇特征}).$$

于是, 如果能证明

$$(X)_\chi \sim \Lambda_\chi/(f),$$

则有

$$G_{\chi^{-1}\omega}(T)\,(\Lambda_\chi/(f)) \sim 0,$$

从而有 $(f) \supset (G_{\chi^{-1}\omega}(T))$, 再比较两者的 λ 不变量便有

$$\mathrm{Char}\,((X)_\chi) = (f) = (G_{\chi^{-1}\omega}(T)),$$

这就是说, 如此便能够证明岩泽主猜想 (定理 10.35) 了. (为了能有 $(X)_\chi \sim \Lambda_\chi/(f)$, 譬如, 只要 $\mathrm{Char}\,((X)_\chi)$ 的生成多项式没有平方因子就可以了. 在迄今已计算过的例子中, $\mathrm{Char}\,((X)_\chi)$ 的生成多项式还没发现有含平方因子的例子.)

因此, 一般情形下设若要证明岩泽主猜想, 那么问题便在于如何处理非循环模 (即不是 $(X)_\chi \sim \Lambda_\chi/(f)$ 的情形). 所谓 Euler 系 (Euler system) 的概念便是为了处理这样的非循环模而想出来的. Stickelberger 元最初叙述的是与 Gauss 和的关系, 而

由 Gauss 和可以构造某些满足 Euler 系公理的数系. 于是便能够处理非循环的 $(X)_\chi$ 了. 对于 Euler 系有兴趣的读者, 请阅读岩泽理论的参考文献 [3] 中的附录.

(e) 与自守形式的关系

在此我们将叙述自守形式的理论在岩泽理论中所起的作用.

作为典型的例子, 我们先应用前一章引进的 Ramanujan 的 Δ 来解释 Ribet 定理 (推论 10.38 的 (2)$\Rightarrow$ (1)) 的证明.

首先, 由于 691 除尽 $\zeta(-11)$, 那么在自守形式的世界里能够有 Ramanujan 的同余式

$$\tau(l) \equiv 1 + l^{11} \pmod{691}$$

(§9.1 定理 9.2). 这里的 l 是任意的素数. 定理 9.2 的证明的重要之处是 B_{12} 被 691 除尽, 就是说可以联想起 $\zeta(-11)$ 被 691 除尽.

其次, 说明一下 Ramanujan 同余式产生非分歧扩域的事实. 为达到此目的的最重要的工具是 Deligne 所构造的相伴于 Δ 的表示.

对于任意的素数 p, Deligne 构造了下面的不可约表示

$$\rho_\Delta : G_\mathbb{Q} = \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_p),$$

它满足如下的条件.

(1) 设 K_Δ 为按 Galois 理论对应于 ρ_Δ 的核的域, 即使得

$$\rho_\Delta : \mathrm{Gal}\,(K_\Delta/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Image}(\rho_\Delta)$$

为同构的域. 这时, 除 p 之外的所有素数均在 $K_\Delta/\mathbb{Q}$ 非分歧. (在 p 处对于所谓的 "crystalline 表示" 而言, 也处于好的状态.)

(2) 设 l 为不等于 p 的素数, Frob_l 为 $\mathrm{Gal}\,(K_{\Delta/}\mathbb{Q})$ 中在 l 的 Frobenius 共轭类. 于是

$$\mathrm{Tr}(\rho_\Delta(\mathrm{Frob}_l)) = \tau(l)$$
$$\det(\rho_\Delta(\mathrm{Frob}_l)) = l^{11}.$$

记对应于 ρ_Δ 的, 具有 $G_\mathbb{Q}$ 作用的一个 2 维 $\mathbb{Q}_p$ 向量空间为 V_Δ. 因为 $G_\mathbb{Q}$ 为紧, 存在具有 $G_\mathbb{Q}$ 作用的秩为 2 的自由 $\mathbb{Z}_p$ 模 A_Δ, 使得 $A_\Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = V_\Delta$. 如果上面表示改成对应于 A_Δ 的表示并仍记为 ρ_Δ, 那么 ρ_Δ 的像便在 $GL_2(\mathbb{Z}_p)$ 中. 于是在下面我们变为了考虑

$$\rho_\Delta : G_\mathbb{Q} \to GL_2(\mathbb{Z}_p).$$

而且还可考虑

$$\rho_\Delta \bmod p : G_\mathbb{Q} \to GL_2(\mathbb{F}_p).$$

由定义, $\rho_\Delta \mod p$ 应满足

$$\mathrm{Tr}\,(\rho_\Delta \mod p(\mathrm{Frob}_l)) = \tau(l) \mod p.$$

在此, 我们试取 $p = 691$. 于是由 Ramanujan 同余式有

$$\begin{aligned}\mathrm{Tr}(\rho_\Delta \mod p(\mathrm{Frob}_l)) &= \tau(l) \mod p\\ &= 1 + l^{11} \mod p\\ \det(\rho_\Delta \mod p(\mathrm{Frob}_l)) &= l^{11} \mod p.\end{aligned}$$

这表明了 A_Δ/p 的半单化 (semi simplification) 为

$$(A_\Delta/p)^{ss} = \mathbb{Z}/p(11) \oplus \mathbb{Z}/p (= \mu_p^{\otimes 11} \oplus \mathbb{Z}/p).$$

其中的 $\mathbb{Z}/p(11)$ 为 Tate 扭转 (参看 (c) 小节). 就是说, $G_\mathbb{Q}$ 以 ω^{11} 作用于 $\mathbb{Z}/p(11)$ 上 (ω: Teichmüller 特征). 因此, $\rho_\Delta \mod p$ 为

$$\rho_\Delta \mod p = \begin{pmatrix}\omega^{11} & * \\ 0 & 1\end{pmatrix} \quad 或者 \quad \begin{pmatrix}\omega^{11} & 0 \\ * & 1\end{pmatrix}$$

中任何一个. 通过适当地选取 A_Δ 则可假设有

$$\rho_\Delta \mod p = \begin{pmatrix}\omega^{11} & 0 \\ * & 1\end{pmatrix}, \ * \neq 0.$$

现设 I_p 为 p 之上的素理想的惯性群, 那么可以证明有

$$\rho_\Delta \mod p|_{I_p} = \begin{pmatrix}\omega^{11} & 0 \\ 0 & 1\end{pmatrix}.$$

于是, 设 L 为按照 Galois 理论对应于 $\mathrm{Ker}(\rho_\Delta \mod p)$ 的域, 即使得

$$\mathrm{Gal}\,(L/\mathbb{Q}) \underset{\rho_\Delta \mod p}{\xrightarrow{\sim}} \mathrm{Image}(\rho_\Delta \mod p)$$

成立的域. 由对于 ρ_Δ 的条件 (1) 知 $L/\mathbb{Q}$ 在所有 p 以外的素数处为非分歧. 因此, 从上所述, $L/\mathbb{Q}(\mu_p)$ 在所有的素理想处均非分歧. 又按照构造知, $\mathrm{Gal}\,(\mathbb{Q}(\mu_p)/\mathbb{Q})$ 以 ω^{-11} 作用于 $\mathrm{Gal}\,(L/\mathbb{Q}(\mu_p))$ 上. 如此一来, Ramanujan 同余式便给出了非分歧扩域. 根据类域论 (参看 §10.2(d)), 我们有

$$A_{\mathbb{Q}(\mu_p)}^{\omega^{-11}} \neq 0.$$

故 Ribet 定理得证明.

下面叙述 Mazur 和 Wiles 的证明思路. 与 Ribet 一样他们也使用相伴于自守形式的表示. 在上面叙述了使用相伴于自守形式的表示能得到非分歧扩域之后, 下面

则采用了下述方针, 即 "非分歧扩域可全部由相伴于自守形式的表示作出". 更准确一点说, 即为了证明

$$\mathrm{Char}\,((X)_\chi) = (G_{\chi^{-1}\omega}(T)) \subset \Lambda_\chi,$$

则要构造出关于 " $\Lambda_\chi/(G_{\chi^{-1}\omega}(T))$ 部分" 的非分歧扩域. 如果这是可能的话, 说明有 $\mathrm{Char}\,((X)_\chi) \subset (G_{\chi^{-1}\omega}(T))$, 那么由 (d) 小节中关于 λ, μ 不变量的讨论, 表明这两者是相等的.

我们来叙述不甚精确的粗略的想法. 如果依照肥田 (Hida) 理论, " 大"Hecke 环 T(由 Hecke 算子生成的环) 满足以下断言. T 为 Λ_χ 上的环, 并有被称为 Eisenstein 理想的理想 I 使得 $T/I \simeq \Lambda_\chi/(G_{\chi^{-1}\omega}(T))$ 成立. 虽然在这种情形下, 还不知道是否存在 T 的 2 维表示

$$\rho : G_{\mathbb{Q}} \to GL_2(T),$$

但与它相近地, 存在有所谓的伪表示 (pseudo-representation). 因此, 与 Δ 的情形一样, 由"$\rho \mod I$" 可以构造关于 T/I 部分, 即 $\Lambda_\chi/(G_{\chi^{-1}\omega}(T))$ 部分的非分歧扩域.

(f) 关于加号部分的岩泽主猜想

对于岩泽主猜想, 由于除了定理 10.35 之外还有另外两个公式化的阐述, 所以最后我们想对此说一下.

让 K_n, K_∞, Λ_{N_0}, Λ_χ 如 (a) 小节所设. 将在 K_∞ 上次数为 p 幂, 并在 p 之上的素理想以外非分歧的所有 Abel 扩域的并记为 M_∞. 令

$$\mathcal{X} = \mathrm{Gal}\,(M_\infty/K_\infty)$$

设 χ 为偶特征 ($\chi(-1)=1$), 并为满足 $\chi \neq \mathbf{1}$ 的第一类特征. 又设

$$(\mathcal{X})_\chi = \mathcal{X} \otimes_{\Lambda_{N_0}} \Lambda_\chi,$$

可以证明 $(\mathcal{X})_\chi$ 为有限生成扭 Λ_χ 模. 此时, 关于 $\mathcal{X}$ 的岩泽主猜想便可表达为

$$\mathrm{Char}\,((\mathcal{X})_\chi) = \left(\frac{1}{2}G_\chi(u(1+T)^{-1}-1)\right).$$

可以证明这与定理 10.35 是等价的.

其次, 设 X_{K_∞} 如 (a) 小节中那样, 那么对于 $\chi \neq \mathbf{1}$ 的第一类偶特征 χ, 我们考虑

$$(X)_\chi = X_{K_\infty} \otimes_{\Lambda_{N_0}} \Lambda_\chi.$$

现在我们来叙述关于 $(X)_\chi$ 的岩泽主猜想.

设 $O_{K_n}^\times$ 为 K_n 的单位群, 定义 $O_{K_n}^\times$ 中的**分圆单位群**(group of cyclotomic units) C_n 为 $C_n = O_{K_n}^\times \cap Z_n$. 这里, 若设 ζ 为 N_0p^n 次本原单位根, 那么 Z_n 表示由 ζ 和

$1-\zeta^a$ $(1 \leqslant a \leqslant N_0p^n-1)$ 生成的 $K_n^\times$ 的子群. 考虑关于范映射的逆极限

$$\begin{aligned}\mathcal{E} &= \varprojlim(O_{K_n}^\times \otimes \mathbb{Z}_p)\\ &\cup\\ \mathcal{C} &= \varprojlim(C_n \otimes \mathbb{Z}_p),\end{aligned}$$

并令

$$(\mathcal{E}/\mathcal{C})_\chi = (\mathcal{E}/\mathcal{C}) \otimes_{\Lambda_{N_0}} \Lambda_\chi.$$

此时, 岩泽主猜想可公式化阐述为

$$\mathrm{Char}\,((X)_\chi) = \mathrm{Char}\,((\mathcal{E}/\mathcal{C})_\chi).$$

可以证明这一等式也与定理 10.35 等价.

小结

10.1 存在以 Dirichlet L 函数在负整数的值插值的 p 进全纯 L 函数 $L_p(s,\chi)$ (准确地说, 是在 $\chi=\mathbf{1}, s=1$ 以外全纯), 并称其为久保田–Leopoldt p 进 L 函数. 使用幂级数 $G_\chi(T)$ 可将 $L_p(s,\chi)$ 写成 $L_p(s,\chi)=G_\chi(u^s-1)$. 另外, 由完备群环 $\Lambda_{N_0}^\sim$ 中的元可构造 $L_p(s,\chi)$.

10.2 对于 $\mathbb{Q}$ 的有限次扩域 K, 令 $K_n = K(\mu_{p^n})$, $K_\infty = \cup K_n$. 设 A_{K_n} 为 K_n 的理想类群的 p-Sylow 群, $X_{K_\infty} = \varprojlim A_{K_n}$ 为按范映射取的逆极限. 此时, X_{K_∞} 是有限生成的扭 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty)/K)]]$ 模.

10.3 设 χ 是具有导子 N 的第一类特征, 且满足 $\chi \neq \omega$, $\chi(-1)=-1$. 又设 $K_\infty = \bigcup_{n>0} \mathbb{Q}(\mu_{Np^n})$, 则关于 X_{K_∞} 的 χ 分量 $(X)_\chi$ 的特征理想, 成立

$$\mathrm{Char}\,((X)_\chi) = \left(\frac{1}{2}G_{\chi^{-1}\omega}(T)\right).$$

称其为岩泽主猜想 (Mazur-Wiles 定理). 这个定理是联系数论对象与 p 进解析对象之间的漂亮的关系式.

10.4 根据以上的理论, 分圆 $\mathbb{Z}_p$ 扩域的理想类群的 p-Sylow 群, 也包括 Galois 群的作用在内, 能够得到统一的理解.

10.5 在数的世界里, 存在这样漂亮的理论真是不可思议.

习题

10.1 设 $X = X_{\mathbb{Q}(\mu_{p^\infty})}$, 并使用与 §10.3(b) 相同的记号. 依照所见 $\zeta(-1), \zeta(-3), \cdots, \zeta(-9)$ 的值, 证明

$$X^{\omega^{p-2}} = X^{\omega^{p-4}} = \cdots = X^{\omega^{p-10}} = 0.$$

10.2　设 r 为正偶数, 以及素数 p 除尽 $\zeta(1-r)$ 的分子.

(1) 证明当 $(2-r-p)\zeta(1-r) \not\equiv (1-r)\zeta(2-r-p) \pmod{p^2}$ 时, 成立

$$A_{\mathbb{Q}(\mu_p)}^{\omega^{1-r}} \simeq \mathbb{Z}/p.$$

(2) 对于 $p=37$, $r=32$, 请确认 (1) 中的关系确实成立.(即确认 §10.0(c) 表 10.2 的关系.)

10.3　设 i 为满足 $1<i<p-1$ 的奇数.

(1) 设伴随于 $G_{\omega^{1-i}}(T)$ 的多项式 (参看 §10.2(a) 命题 10.19) 为一次式 $T-\alpha$. 令 $\mathrm{ord}_p(\alpha)=a$ 时, 证明有

$$A_{\mathbb{Q}(\mu_{p^n})}^{\omega^i} \simeq \mathbb{Z}/p^{a+n-1}.$$

(2) 假定伴随于 $G_{\omega^{1-i}}(T)$ 的多项式为二次式 $(T-\alpha)(T-\beta)$ $(\alpha,\beta\in\mathbb{Z}_p)$, 且 $1=\mathrm{ord}_p(\alpha)<\mathrm{ord}_p(\beta)$. 此时, 请求出 Abel 群 $A_{\mathbb{Q}(\mu_{p^n})}^{\omega^i}$ 的结构. (如同在问题 4 所说的, 还不知道有像 (2) 那样的 $G_{\omega^{1-i}}(1-T)$ 的例子. 但是, 对于满足某种条件的特征 χ, 如果 $G_{\chi^{-1}\omega}(T)$ 能写成上述形式, 以同样的方法, 是可以求出 $A_{K_n}^{\chi}$ 作为 Abel 群的结构的. §10.0(c) 中所叙述过的例子 $\mathbb{Q}(\sqrt{-1399},\sqrt{-3})$ 的分圆 $\mathbb{Z}_p$ 扩域的理想类群的构造便是这样计算的.)

10.4　(1) 设 p 为奇素数, χ 为第一类特征, 且满足 $\chi\neq\omega$, $\chi(-1)=-1$, 并且 $\mathrm{Image}(\chi)$ 的阶与 p 互素. 又设, 根据 Galois 理论对应于 χ 的核的域为 F. 也就是说 $\chi:\mathrm{Gal}(F/\mathbb{Q})\hookrightarrow\overline{\mathbb{Q}}_p^{\times}$ 为单射. 另外, 假定在 $F/\mathbb{Q}$ 上 p 不可分解. 对于 χ, 让 O_χ, K, K_n, K_∞ 为在 §10.3(a) 中所设那样, 并令 $G_0=\mathrm{Gal}(K/F)$. 有分解 $\mathrm{Gal}(K_n/F)=G_0\times\mathrm{Gal}(K_n/K)$, 并将 G_0 看作了 $\mathrm{Gal}(K_n/F)$ 的子群. 记对应于 G_0 的 K_n/F 的中间域为 F_n $(F_n=(K_n)^{G_0})$.

根据 $\mathrm{Gal}(F_n/\mathbb{Q})=\mathrm{Gal}(F/\mathbb{Q})\times\mathrm{Gal}(F_n/F)$, 将 $\mathrm{Gal}(F/\mathbb{Q})$ 看作 $\mathrm{Gal}(F_n/\mathbb{Q})$ 的子群, 从而将 $\mathrm{Gal}(F_n/\mathbb{Q})$ 模看作 $\mathrm{Gal}(F/\mathbb{Q})$ 模.

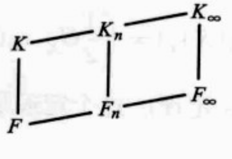


图 10.4

又按照 χ 将 O_χ 看作 $\mathrm{Gal}(F/\mathbb{Q})$ 模, 并令

$$A_{F_n}^{\chi}=A_{F_n}\otimes_{\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}O_\chi$$
$$A_{K_n}^{\chi}=A_{K_n}^{\mathrm{Gal}(K_n/F_n)}\otimes_{\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}O_\chi.$$

此时, 证明自然映射

$$A_{F_n}^{\chi}\to A_{K_n}^{\chi}$$

为同构.

(2) 证明 $\#A_F^{\chi}=\#(O_\chi/L(0,\chi^{-1}))$.

第十一章　自守形式 (II)

根据我们在第九章所见，自守形式原本指的是上半复平面上的单变量全纯的自守形式，但后来，则对自守形式进行了各式各样的推广，包括了非全纯的以及多变量的情形，虽然如此，还是有这样的统一观点，即通过掌握群上的函数来得到自守形式．于是自守形式与群表示论之间的关联便凸显出来了．称通过自守形式给出的表示为自守表示，对数论而言它是个很具兴趣的对象．

在这一章里我们将介绍自守形式与表示论之间的关系．这是以 Ramanujan 的 $\tau(n)$ 的三种表示典型地表现出来的．另外，还要谈及在表示论中表现出重要的对偶性的 Poisson 求和公式以及作为它的推广的 Selberg 迹公式 (形如 $\sum\limits_{m} M(m) = \sum\limits_{w} W(w)$ 的公式) 在数论中的应用．例如，表现在 ζ 函数的函数方程中的对偶性 (Poisson 求和公式 (Selberg 迹公式)) 等很多的地方．

最后还将介绍与自守表示有关的 Langlands 猜想．这是个试图推广类域论的猜想，是 Galois 群的表示与自守表示的对应，含有某种对偶性的意思．Langlands 猜想可以称做非交换类域论猜想．Fermat 猜想的证明是通过证明 Langlands 猜想的一部分而得以完成的．自此，Langlands 猜想的一般性的证明便是个有待解决的问题，长时间以来被认为给出了数论的指导纲领．

§11.1 自守形式与表示论

(a) $\tau(n)$ 的三种表达与表示论

我们在第九章看到, Ramanujan 所考虑的

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

成为自守形式的数论研究的开端. 就像在 §9.1 所证明的, 出现在上式的系数 $\tau(n)$ 具有如下的表达式

$$\tau(n) = \sigma_{11}(n) + \frac{691}{756}\left(-\sigma_{11}(n) + \sigma_5(n) - 252\sum_{m=1}^{n-1}\sigma_5(m)\sigma_5(n-m)\right) \tag{11.1}$$

(参看 (9.8) 式). 其中, $\sigma_k(n) = \sum_{d|n} d^k$. 从它可推导出 Ramanujan 同余式 $\tau(n) \equiv \sigma_{11}(n) \mod 691$ 的意义而言这是个重要的表达式. 这个等式是由与等式

$$\Delta = \frac{E_{12} - E_6^2}{1008 \cdot 756}$$

的 Fourier 系数进行比较得到的, $E_k(z)$ 的 Fourier 系数的计算基础是公式 (9.14)(Lipschitz 公式), 像在 §11.2 将要说明的那样, 这恰好是 Poisson 求和公式. 在这个意义上, 我们认为 (11.1) 的表达式是 Poisson 求和公式 (对于 $\mathbb{Z} \subset \mathbb{R}$ 的群组的 Selberg 迹公式) 的表示论的应用.

另外, 对 $\tau(n)$ 还有其他各种各样的表达方式. (第九章的习题 9.1(3) 也是这样的.) 我们举出其中的两个. 首先, 物理学家 Dyson(1968 年) 给出了如下的表达式:

$$\tau(n) = \sum_{\substack{(a,b,c,d,e)\in\mathbb{Z}^5 \\ (a,b,c,d,e)\equiv(1,2,3,4,5) \mod 5 \\ a+b+c+d+e=0 \\ a^2+b^2+c^2+d^2+e^2=10n}} \frac{(a-b)(a-c)(a-d)(a-e)(b-c)(b-d)(b-e)(c-d)(c-e)(d-e)}{1!2!3!4!}. \tag{11.2}$$

这里的和是有限和, 例如, 当 $n=1$ 时只有 $(a,b,c,d,e) = (1,2,-2,-1,0)$, 故 $\tau(1)=1$. 为此, 可以考虑在级数

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{m=-\infty}^{\infty}(-1)^m q^{\frac{3m^2-m}{2}} \quad \text{(Euler的五角数定理, 1750年)}$$

以及

$$\prod_{n=1}^{\infty}(1-q^n)^3=\sum_{m=0}^{\infty}(-1)^m(2m+1)q^{\frac{m^2+m}{2}} \quad (\text{Jacobi公式}, 1829\text{年})$$

($\dfrac{3m^2-m}{2}$为 5 角数, $\dfrac{m^2+m}{2}$ 为 3 角数) 上取 24 次幂. 这个 Dyson 表达式到了 20世纪70 年代被 MacDonald 的应用以及 Kac 由无限维 Lie 环表示论(指标公式)推出从而得以弄清. 这也是表示论的应用.

下面的表达式是由 Selberg(1952年) 得到的:

$$(11.3) \qquad \tau(n)=-\sum_{0\leqslant m<2\sqrt{n}}{}' \; H(m^2-4n)\frac{\eta_m^{11}-\bar{\eta}_m^{11}}{\eta_m-\bar{\eta}_m}-\sum_{\substack{d\mid n\\ d\leqslant\sqrt{n}}}{}' d^{11}+\frac{11}{12}\delta(\sqrt{n})n^5.$$

其中, $\delta(\sqrt{n})$ 表示当 n 为平方数时为 1 否则为 0, $\sum'$ 表示在取和范围的边界处 (即 $m=0$ 以及 $d=\sqrt{n}$ 处) 要乘以权 $\frac{1}{2}$, 又

$$\eta_m=\frac{m+i\sqrt{4n-m^2}}{2},$$

而 $H(d)$ 则是判别式 $d<0$ 的二次型的加权类数. 例如, $H(-4)=\frac{1}{2}$, $H(-3)=\frac{1}{3}$. (这里给出的二次型的类数稍许推广了虚二次域的类数.) Selberg 给出的这个表达式是由 Selberg 迹公式对 $SL_2(\mathbb{Z})\subset SL_2(\mathbb{R})$ (或者 $SL_2(\mathbb{Q})\subset SL_2(\mathbb{A})$) 推导出来的. Selberg 迹公式将在 §11.3 中讲解. 仅就所见到的这样的 $\tau(n)$ 的表达式而言, 表示论在自守形式上的应用有很多.

(b) 从自守形式到自守表示

从对于模群 $SL_2(\mathbb{Z})$ 的自守形式来构造群 $SL_2(\mathbb{R})$ 上的自守形式, 如果使用上半平面的表示

$$H=SL_2(\mathbb{R})/SO(2),$$

则比较简单. 具体地说, 对于全纯自守形式 $f\in M_k(SL_2(\mathbb{Z}))$ 令

$$\varphi_f(g)=f(gi)j(g,i)^{-k},$$

则给出了函数

$$\varphi_f: SL_2(\mathbb{R})\to\mathbb{C},$$

其在 $SL_2(\mathbb{Z})$ 下左不变, 即对于所有 $\gamma\in SL_2(\mathbb{Z})$ 成立

$$\varphi_f(\gamma g)=\varphi_f(g).$$

因此, 可看作

$$\varphi_f: SL_2(\mathbb{Z})\backslash SL_2(\mathbb{R})\to\mathbb{C}.$$

并且, 如果 $f \in S_k(SL_2(\mathbb{Z}))$, 则有

$$\varphi_f \in L^2(SL_2(\mathbb{Z})\backslash SL_2(\mathbb{R}))$$

来补充一点计算. 在上面的构成中, $i=\sqrt{-1}\in H$, 对于一般的 $z\in H$ 与 $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbb{R})$, 有

$$gz=\frac{az+b}{cz+d},$$
$$j(g,z)=cz+d.$$

对于 g_1, $g_2\in SL_2(\mathbb{R})$ 经简单计算知道成立

$$(g_1g_2)z=g_1(g_2z),$$
$$j(g_1g_2,z)=j(g_1,g_2z)j(g_2,z)$$

(参看 §9.6). 利用它们, 对于 $g\in SL_2(\mathbb{R})$, $\gamma\in SL_2(\mathbb{Z})$ 有

$$\begin{aligned}\varphi_f(\gamma g)&=f(\gamma gi)j(\gamma g,i)^{-k}\\&=f(gi)\cdot j(\gamma,gi)^k j(\gamma g,i)^{-k}\\&=f(gi)j(g,i)^{-k}\\&=\varphi_f(g).\end{aligned}$$

另外, 当 $f\in W_r(SL_2(\mathbb{Z}))$ 时, 若简单地令

$$\varphi_f(g)=f(gi),$$

则有

$$\varphi_f: SL_2(\mathbb{Z})\backslash SL_2(\mathbb{R})\to\mathbb{C}.$$

更一般地, 在 Siegel 自守形式时 (参看 §9.7), 譬如若 $f\in M_k(Sp_n(\mathbb{Z}))$, 并令

$$\varphi_f: Sp_n(\mathbb{R})\to\mathbb{C}$$

为

$$\varphi_f(g)=f(gi)j(g,i)^{-k},$$

则 φ_f 为 $Sp_n(\mathbb{Z})$ 左不变, 从而有

$$\varphi_f: Sp_n(\mathbb{Z})\backslash Sp_n(\mathbb{R})\to\mathbb{C}.$$

然而, 对于 $g=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in Sp_n(\mathbb{R})$, 有

$$gi=(Ai+B)(Ci+D)^{-1}$$
$$j(g,i)=\det(Ci+D).$$

在此, 是以 Siegel 上半空间的表示 $H_n = Sp_n(\mathbb{R})/U(n)$ 为背景的.

这样, 在一般情形, 当有群组 $G \supset \Gamma$, 而 G 上的函数

$$\varphi : G \to \mathbb{C}$$

为 Γ 左不变时, 便称 φ 为关于 Γ 的自守形式.

下面, 我们考虑局部紧群 G 及其离散子群 Γ 形成的组. 这样的例子相当丰富, 出现在通常的自守形式理论中的

$$G = SL_2(\mathbb{R}) \supset SL_2(\mathbb{Z}) = \Gamma$$

以及

$$G = Sp_n(\mathbb{R}) \supset Sp_n(\mathbb{Z}) = \Gamma$$

等将 Γ 作为同余子群形成了这样的组, 此外对于整体域 K, 设 $\mathbb{A}_K$ 为阿代尔环 (第六章), 则

$$G = SL_2(\mathbb{A}_K) \supset SL_2(K) = \Gamma$$

$$G = Sp_n(\mathbb{A}_K) \supset Sp_n(K) = \Gamma$$

$$G = GL_n(\mathbb{A}_K) \supset GL_n(K) = \Gamma$$

等形成的 (G, Γ) 也是这样的例子. 其他的, 对于 $n = 1, 2, 3, \cdots$ 的加法群组

$$G = \mathbb{R}^n \supset \mathbb{Z}^n = \Gamma$$

$$G = \mathbb{A}_K^n \supset K^n = \Gamma$$

等也构成这种例子.

再有, 当这样的群组 (G, Γ) 给出后, G 的表示则可像下面那样自然地得到. 对于一般的 $\psi \in L^2(\Gamma \backslash G)$ 与 $g \in G$, ψ 的右移 ψ_g 按

$$\psi_g(x) = \psi(xg)$$

确定. 于是 G 在 $L^2(\Gamma \backslash G)$ 上以

$$\begin{array}{rcl} R : L^2(\Gamma \backslash G) & \longrightarrow & L^2(\Gamma \backslash G) \\ \Psi & & \Psi \\ \psi & \longmapsto & \psi_g \end{array}$$

的形式作用, 从而形成了群 G 的表示

$$G \to \mathrm{Aut}_{\mathbb{C}}(L^2(\Gamma \backslash G)),$$

并称之为**右正则表示** (right regular representation). 称这个表示的子表示为**自守表示** (automorphic representation).

特别地, 设给出了一个自守形式

$$\varphi \in L^2(\Gamma\backslash G).$$

此时, 设由 $\{\varphi_g \mid g \in G\}$ 张成的 $L^2(\Gamma\backslash G)$ 的子空间为 V_φ, G 也作用于 V_φ, 并诱导了表示

$$G \to \mathrm{Aut}_{\mathbb{C}}(V_\varphi).$$

这是由自守形式 φ 生成的自守表示.

最基本的自守表示是, 对于整体域 K 的 $L^2(GL_n(K)\backslash GL_n(\mathbb{A}_K))$(准确地说是附带有关于 $GL_n(\mathbb{A}_K)$ 的中心变换条件) 的子 (不可约) 表示 π. 此时通过 π 的张量积分解 $\pi = \bigotimes_v \pi_v$ (v 过 K 的素点, π_v 为 $GL_n(K_v)$ 的表示), 构成了标准的 n 次 Euler 积 $L(s,\pi)$:

$$L(s,\pi) = \prod_{v<\infty} L(s,\pi_v) = \prod_{v<\infty} \det(1 - t_v N(v)^{-s})^{-1}.$$

其中 $t_v \in GL_n(\mathbb{C})$ 为对角型矩阵 (半单共轭类). 此时 Ramanujan 猜想的类比是 "$t_v \in U(n)$ (t_v 的所有特征值的绝对值为 1)". 当 $n=1$ 时, π 成为

$$GL_1(K)\backslash GL_1(\mathbb{A}_K) = C_K$$

的特征, $L(s,\pi)$ 为在第七章中出现的一次 L 函数. 另外, 在 $n=2$ 的情形中, 譬如对于由 Ramanujan 的 Δ 构成的表示 $\pi = \pi_\Delta$, 有

$$L(s,\pi) = L\left(s + \frac{11}{2}, \Delta\right),$$

其中的平移并不重要, 而其本质上与原来的 L 函数一致, 同样的还有由 Hecke 算子的共有特征函数给出的情形. 一般地, $L(s,\pi)$ 可解析延拓为整个 s 平面上的亚纯函数, 并可证明有 $s \leftrightarrow 1-s$ 这种函数方程 (Godement–Jacquet, 1972年).

再者, 业已知道, $L(s,\pi)$ 在 $\mathrm{Re}(s) \geqslant 1$ 中不具有零点 (Jacquet–Shalika, 1976年). 它推广了证明素数定理 (第七章) 所必需的事实 "在 $\mathrm{Re}(s) \geqslant 1$ 有 $\zeta(s) \neq 0$". 其中, $\mathrm{Re}(s) = 1$ 上不具有零点的断言就像在第九章 (§9.4(b)) 中给出了在 $\zeta(s)$ 情形的另一种证明那样, 也可由观察一个大的群 $GL_{n+1}(\mathbb{A}_K)$ 的 Eisenstein 级数的 "常数项" 而得到证明.

另外, 还可考虑与 §9.3(b) 的逆定理同样的问题. "当给出了 $GL_n(K_v)$ 的表示 π_v 时, $\pi = \bigotimes_v \pi_v$ 是自守表示的条件可由 n 次 Euler 乘积

$$L(s,\pi) = \prod_v L(s,\pi_v)$$

的性质来阐述". 在一般情形下, 我们知道 "π 成为自守表示的条件是 $L(s,\pi)$ 具有好的解析性质 (解析延拓与函数方程)" 这种类型的逆定理. 但是现在是对于 GL_n 的逆定理, 按照 $GL_m (m \leqslant n-1)$ 的自守表示 ω 的 nm 次扭的 Euler 积 $L(s,\pi\otimes\omega)$ 必须全都满足好的解析性质才行 (Piatetski–Shapiro; $n \leqslant 3$ 时只要 $m=1$ 即可).

§11.2 Poisson 求和公式

(a) Poisson 求和公式的发端

Poisson 求和公式 (Poisson summation formula) 原本是指对于 $\mathbb{R}$ 上适当的函数 $f(x)$ 所成立的等式

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n). \tag{11.4}$$

其中,

$$\hat{f}(y) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i y x} dx$$

为 **Fourier 变换** (Fourier transform). 等式 (11.4) 是由 Fourier 级数理论按下面方法推导出的 (在此只是形式的处理, 不涉及收敛性问题). 首先考虑

$$F(x) = \sum_{n=-\infty}^{\infty} f(x+n).$$

由于有 $F(x) = F(x+1)$ 这样的周期性, 故可展成 Fourier 级数, 并记为

$$F(x) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n x}.$$

其中

$$\begin{aligned} a_n &= \int_0^1 F(x) e^{-2\pi i n x} dx \\ &= \int_{-\infty}^{\infty} f(x) e^{-2\pi i n x} dx \\ &= \hat{f}(n). \end{aligned}$$

因此作为 $F(x)$ 的两种表达式我们得到了等式

$$\sum_{n=-\infty}^{\infty} f(x+n) = \sum_{n=-\infty}^{\infty} \hat{f}(n) e^{2\pi i n x}. \tag{11.5}$$

其中, 设 $x=0$ 则得到了 (11.4). 这样的 Poisson 求和公式是计算某个量的两种方式而后将其相等得到的. 还有, 若在 (11.5) 中设 $x=a$ 并使用 $f_a(x) = f(a+x)$, 则由于 $\widehat{f_a}(y) = \hat{f}(y) e^{2\pi i a y}$, 故再次得到 (11.4).

迄今所出现的 Lipschitz 公式 (第九章的 (9.14) 式) 以及 ϑ 的变换公式 (§7.2, §7.5) 都是这个 Poisson 求和公式的特殊情形. 譬如, Lipschitz 公式, 对于 $\mathrm{Im}\tau > 0$ 令

$$f(x) = \frac{1}{(x+\tau)^k},$$

从而由

$$\hat{f}(y)=\begin{cases}\dfrac{(-2\pi i)^k}{(k-1)!}y^{k-1}e^{2\pi iy\tau} & (y>0)\\ 0 & (y\leqslant 0)\end{cases}$$

即得. 又令

$$f(x)=\frac{1}{|x+\tau|^{2s}},$$

那么则得到了 Lipschitz 公式的非全纯形式

$$\sum_{n=-\infty}^{\infty}\frac{1}{|\tau+n|^{2s}}=\frac{\Gamma_{\mathbb{R}}(2s-1)}{\Gamma_{\mathbb{R}}(2s)}(\mathrm{Im}\tau)^{1-2s}+\frac{2}{\Gamma_{\mathbb{R}}(2s)}(\mathrm{Im}\tau)^{\frac{1}{2}-s}\sum_{\substack{m=-\infty\\ m\neq 0}}^{\infty}|m|^{s-\frac{1}{2}}K_{s-\frac{1}{2}}(2\pi|m|\mathrm{Im}\tau).$$

其中 $\Gamma_{\mathbb{R}}(s)=\pi^{-\frac{s}{2}}\Gamma\left(\dfrac{s}{2}\right)$, 而 $K_s(z)$ 为变形 Bessel 函数 (参看 §9.4). 利用它可以进行实解析 Eisenstein 级数的 Fourier 系数的计算 (参看 §9.4(a)).

至于 ϑ 的变换公式, 对于 $t>0$ 只要取

$$f(x)=e^{-\pi tx^2}$$

即可. 于是由

$$\hat{f}(y)=\frac{1}{\sqrt{t}}e^{-\frac{\pi y^2}{t}}$$

得到了

$$\sum_{n=-\infty}^{\infty}e^{-\pi tn^2}=\frac{1}{\sqrt{t}}\sum_{m=-\infty}^{\infty}e^{-\pi\frac{m^2}{t}}$$

以及

$$\sum_{n=-\infty}^{\infty}e^{-\pi t(x+n)^2}=\frac{1}{\sqrt{t}}\sum_{m=-\infty}^{\infty}e^{-\pi\frac{m^2}{t}+2\pi imx}.$$

(b) 广义 Poisson 求和公式

原本的 Poisson 求和公式是相对于群组 $\mathbb{R}\supset\mathbb{Z}$ 的. 若考虑交换群 (Abel 群) 组 $G\supset\Gamma$ (G 为局部紧的交换群, Γ 为其离散子群) 的情形, 则得到广义的 Poisson 求和公式:

$$\sum_{\gamma\in\Gamma}f(\gamma)=\sum_{\pi\in\widehat{\Gamma\backslash G}}\hat{f}(\pi). \tag{11.6}$$

这里的 f 为 G 上适当的函数, $\widehat{\Gamma\backslash G}$ 是商群 $\Gamma\backslash G$ 的 (酉) 特征全体 (形成交换群), 而

$$\hat{f}(\pi)=\int_G f(x)\pi^{-1}(x)dx$$

为 Fourier 变换. 但由于 Γ 为交换群 G 的离散子群, 从而 $\Gamma\backslash G$ 是个紧群, 以 $\mathrm{vol}(\Gamma\backslash G) = 1$ 使测度正规化.

广义 Poisson 求和公式的证明可以像 $\mathbb{R} \supset \mathbb{Z}$ 的情形一样如下地进行: 令

$$F(x) = \sum_{\gamma \in \Gamma} f(\gamma x),$$

F 为 $\Gamma\backslash G$ 上的函数, 且可按 $\widehat{\Gamma\backslash G}$ 的元展开为 Fourier 级数, 记其为

$$F(x) = \sum_{\pi \in \widehat{\Gamma\backslash G}} c(\pi)\pi(x).$$

这里, 由于

$$\begin{aligned} c(\pi) &= \int_{\Gamma\backslash G} F(x)\pi^{-1}(x)dx \\ &= \int_G f(x)\pi^{-1}(x)dx \\ &= \hat{f}(\pi), \end{aligned}$$

故有

$$\sum_{\gamma \in \Gamma} f(\gamma x) = F(x) = \sum_{\pi \in \widehat{\Gamma\backslash G}} \hat{f}(\pi)\pi(x).$$

那么只要令 $x = 1$ 就可以了.

譬如, 当 $G = \mathbb{R}^n \supset \mathbb{Z}^n = \Gamma$ 时, 将

$$\widehat{\Gamma\backslash G} = \mathbb{Z}^n$$

看为相同, 那么对于 $\mathbb{R}^n$ 上的函数 f 成立等式

$$\sum_{m_1,\cdots,m_n=-\infty}^{\infty} f(m_1,\cdots,m_n) = \sum_{m_1,\cdots,m_n=-\infty}^{\infty} \hat{f}(m_1,\cdots,m_n).$$

其中的

$$\hat{f}(y_1,\cdots,y_n) = \int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} f(x_1,\cdots,x_n)e^{-2\pi i(y_1x_1+\cdots+y_nx_n)}dx_1\cdots dx_n.$$

利用它可以得到由多元二次型构造的 ϑ 级数的自守性, 以及某类 ζ (Epstein ζ) 的函数方程.

作为二元 (n=2) Poisson 求和公式应用的例子, 我们来给出 §9.4 中进行的实解析 Eisenstein 级数的解析延拓以及函数方程 ($s \leftrightarrow 1-s$) 的另一个证明 (但不包括 Fourier 展开).

首先, 对于 $\mathrm{Im}z > 0$ 与 $t > 0$ 令

$$\theta_z(t) = \sum_{m,n=-\infty}^{\infty} e^{-\pi\left(\frac{|mz+n|^2}{y}\right)t},$$

按照二元 Poisson 求和公式, 成立 ϑ 的变换公式

$$\theta_z\left(\frac{1}{t}\right) = t\theta_z(t).$$

特别地, 对于 $\mathrm{Re}\,(s) > 1$ 得知

$$\begin{aligned}
\widehat{E}(s,z) &= \widehat{\zeta}(2s)E(s,z) \\
&= \pi^{-s}\Gamma(s)\cdot\frac{1}{2}\sum_{m,n=-\infty}^{\infty}{}' \frac{y^s}{|mz+n|^{2s}} \\
&= \frac{1}{2}\int_0^\infty (\theta_z(t)-1)t^{s-1}dt \\
&= \frac{1}{2}\int_1^\infty (\theta_z(t)-1)t^{s-1}dt + \frac{1}{2}\int_0^1 (\theta_z(t)-1)t^{s-1}dt.
\end{aligned}$$

现在, 由于

$$\begin{aligned}
\int_0^1 (\theta_z(t)-1)t^{s-1}dt &= \int_0^1 \left(\left(\theta_z(t)-\frac{1}{t}\right)+\left(\frac{1}{t}-1\right)\right)t^{s-1}dt \\
&= \int_0^1 \left(\theta_z(t)-\frac{1}{t}\right)t^{s-1}dt + \int_0^1 \left(t^{s-2}-t^{s-1}\right)dt \\
&= \int_1^\infty \left(\theta_z\left(\frac{1}{t}\right)-t\right)t^{-s}\frac{dt}{t} + \left[\frac{t^{s-1}}{s-1}-\frac{t^s}{s}\right]_0^1 \\
&= \int_1^\infty (t\theta_z(t)-t)t^{-s}\frac{dt}{t} + \frac{1}{s-1} - \frac{1}{s} \\
&= \int_1^\infty (\theta_z(t)-1)t^{1-s}\frac{dt}{t} + \frac{1}{s(s-1)}
\end{aligned}$$

故有

$$\widehat{E}(s,z) = \frac{1}{2}\int_1^\infty (\theta_z(t)-1)(t^s+t^{1-s})\frac{dt}{t} + \frac{1}{2s(s-1)},$$

由此可得到解析延拓和函数方程. 再有, 从这个表达式可以得知 $\widehat{E}(s,z)$ 只在 $s=0,1$ 具有一阶极点, 其留数分别为 $-\frac{1}{2}, \frac{1}{2}$. 这个结果在 §9.4(a) 中是通过计算 $\widehat{E}(s,z)$ 的 Fourier 展开得到的: 观察 Laurent 展开, 于是有

$$\begin{aligned}
&(\text{在}s=0) \quad \widehat{\zeta}(2s)y^s = -\frac{1}{2s} + (\text{全纯项}), \\
&(\text{在}s=1) \quad \widehat{\zeta}(2s-1)y^{1-s} = \frac{1}{2s-2} + (\text{全纯项}).
\end{aligned}$$

此外, 从 Fourier 展开来看, 似乎 $s=\frac{1}{2}$ 也是极点, 但考虑在 $s=\frac{1}{2}$ 处的 Laurent 展开, 有

$$\widehat{\zeta}(2s)y^s=\frac{y^{\frac{1}{2}}}{2s-1}+(\text{全纯项})$$

$$\widehat{\zeta}(2s-1)y^{1-s}=-\frac{y^{\frac{1}{2}}}{2s-1}+(\text{全纯项})$$

所见到的极点相互消去从而在 $s=\frac{1}{2}$ 为全纯.

(c) Poisson 求和公式的应用: ζ 积分

Poisson 求和公式对于整体域 K

$$G=\mathbb{A}_K\supset K=\Gamma$$

和加群

$$G=M_n(\mathbb{A}_K)\supset M_n(K)=\Gamma$$

的情形也成立. 于是可以得到像 §7.5 的命题 7.13(1) 那样的 ϑ 的变换公式. 若使用它, 则能得到 $GL_n(\mathbb{A}_K)$ 的自守表示 π 的 L 函数 $L(s,\pi)$ 的积分表示, 并能够证明 $s\leftrightarrow 1-s$ 这样的函数方程 (Godement–Jacquet, 1972年). 这是在第七章所见到的 $n=1$ 情形的推广. 再说, 在 GL_n 情形使用的 ζ 积分为以下形式:

$$\begin{aligned}Z(s,f,\Phi)&=\int_{GL_n(\mathbb{A}_K)}\Phi(x)f(x)|\det x|^s d^\times x\\&=\prod_v Z(s,f_v,\Phi_v).\end{aligned}$$

其中,

$$f:GL_n(K)\backslash GL_n(\mathbb{A}_K)\to\mathbb{C}$$

为自守形式, 并设 Φ 为 $M_n(\mathbb{A}_K)$ 上适当的函数 (相应于 f 而决定). 此时, 若使用 Poisson 求和公式

$$\sum_{\xi\in M_n(K)}\Phi(a\xi)=|a|^{-n^2}\sum_{\xi\in M_n(K)}\widehat{\Phi}(a^{-1}\xi)$$

(实际使用时在两端对 ξ 按次数分类), 则得到了函数方程

$$Z(s,f,\Phi)=Z(n-s,\check{f},\widehat{\Phi}).$$

而

$$\check{f}(g)=f(g^{-1}),$$

$\widehat{\Phi}$ 为 Φ 的 "Fourier 变换":

$$\widehat{\Phi}(y)=\int_{M_n(\mathbb{A}_K)}\Phi(x)\psi(\mathrm{Tr}\,(xy))dx.$$

这里的 ψ 取作 $\mathbb{A}_K/K$ 的一个非平凡特征. 在这个函数方程中, 若适当地选取 Φ, 则 $Z\left(s+\dfrac{n-1}{2}, f, \Phi\right)$ 本质上就是 $L(s,\pi_f)$, 从而得到了 GL_n 的自守 L 函数的函数方程.

§11.3 Selberg 迹公式

(a) 从 Poisson 求和公式到 Selberg 迹公式

Poisson 求和公式尽管限定在交换群组 $G\supset\Gamma$ 的情形, 然而还可以推广到不限于交换的一般群组 $G\supset\Gamma$, 即由 Selberg(1952 年左右) 所发现的 **Selberg 迹公式** (Selberg trace formula). (因此, Poisson 求和公式是 Selberg 迹公式的一部分, 可以由 Selberg 迹公式总括起来讨论, 然而由于历史的原因仍然沿用 Poisson 求和公式的名称.)

在这里, 设 G 为紧群并具有幺模 (具有双边不变 Haar 测度), Γ 为 G 的离散子群, 从而 $\Gamma\backslash G$ 为紧. 此时, 对于 G 上适当的函数 $f: G\to\mathbb{C}$ 的 Selberg 迹公式为

$$\sum_{[\gamma]\in\mathrm{Conj}\,(\Gamma)} \mathrm{vol}\,(\Gamma_\gamma\backslash G_\gamma)\int_{G_\gamma\backslash G} f(x^{-1}\gamma x)dx = \sum_{\pi\in\widehat{G}} m(\pi)\mathrm{trace}\,(\pi(f)). \tag{11.7}$$

左端是 Γ 的**共轭类全体**(conjugacy classes) $\mathrm{Conj}\,(\Gamma)$ 上的和 ($[\gamma]$ 为包含 γ 的共轭类), 而

$$\Gamma_\gamma = \{g\in\Gamma \mid g\gamma=\gamma g\}$$
$$G_\gamma = \{g\in G \mid g\gamma=\gamma g\}$$

为中心化群. 右端为对 G 的不可约(酉)**表示的等价类全体** (equivalence classes of representations) $\widehat{G}$ 取和, 而

$$\pi(f): L^2(\Gamma\backslash G)\to L^2(\Gamma\backslash G)$$

是由

$$(\pi(f)\varphi)(x) = \int_G f(y)(\pi(y)\varphi)(x)dy$$

决定的算子, $m(\pi)$ 为将 G 在 $L^2(\Gamma\backslash G)$ 上的右正则表示

$$R: G\to \mathrm{Aut}_{\mathbb{C}}(L^2(\Gamma\backslash G))$$

分解为不可约表示

$$R\cong\bigoplus_{\pi\in\widehat{G}} m(\pi)\pi$$

时的 π 的**重数** (multiplicity) (大于或等于零的整数).

下面进行证明. 首先, 我们回想起右正则表示 R 是说, 对于 $y \in G$ 以及 $\varphi \in L^2(\Gamma\backslash G)$ 有

$$(R(y)\varphi)(x) = \varphi(xy).$$

现令 $L^2(\Gamma\backslash G)$ 上的算子 $R(f)$ 为

$$R(f) = \int_G f(y)R(y)dy.$$

具体地,

$$\begin{aligned}(R(f)\varphi)(x) &= \int_G f(y)(R(y)\varphi)(x)dy \\ &= \int_G f(y)\varphi(xy)dy \\ &= \int_G f(x^{-1}y)\varphi(y)dy \\ &= \int_{\Gamma\backslash G}\left(\sum_{\gamma\in\Gamma} f(x^{-1}\gamma y)\varphi(\gamma y)\right)dy \\ &= \int_{\Gamma\backslash G}\left(\sum_{\gamma\in\Gamma} f(x^{-1}\gamma y)\right)\varphi(y)dy.\end{aligned}$$

于是当令

$$K(x,y) = \sum_{\gamma\in\Gamma} f(x^{-1}\gamma y)$$

(称之为**核函数** (kernel function)) 时, 便有

$$(R(f)\varphi)(x) = \int_{\Gamma\backslash G} K(x,y)\varphi(y)dy,$$

并由积分算子的理论得到

$$\begin{aligned}\mathrm{Tr}\,(R(f)) &= \int_{\Gamma\backslash G} K(x,x)dx \\ &= \int_{\Gamma\backslash G}\left(\sum_{\gamma\in\Gamma} f(x^{-1}\gamma x)\right)dx \\ &= \int_{\Gamma\backslash G}\left(\sum_{[\gamma]\in\mathrm{Conj}\,(\Gamma)}\ \sum_{\alpha\in\Gamma_\gamma\backslash\Gamma} f(x^{-1}\alpha^{-1}\gamma\alpha x)\right)dx\end{aligned}$$

$$
\begin{aligned}
&= \sum_{[\gamma]\in \mathrm{Conj}\,(\Gamma)} \int_{\Gamma\backslash G} \left(\sum_{\alpha\in\Gamma_\gamma\backslash\Gamma} f(x^{-1}\alpha^{-1}\gamma\alpha x) \right) dx \\
&= \sum_{[\gamma]\in \mathrm{Conj}\,(\Gamma)} \int_{\Gamma_\gamma\backslash G} f(u^{-1}\gamma u)du \\
&= \sum_{[\gamma]\in \mathrm{Conj}\,(\Gamma)} \mathrm{vol}\,(\Gamma_\gamma\backslash G_\gamma) \int_{G_\gamma\backslash G} f(x^{-1}\gamma x)dx.
\end{aligned}
$$

另一方面, 由于有

$$R \cong \bigoplus_{\pi\in\widehat{G}} m(\pi)\pi,$$

故

$$R(f) \cong \bigoplus_{\pi\in\widehat{G}} m(\pi)\pi(f).$$

于是有

$$\mathrm{Tr}\,(R(f)) = \sum_{\pi\in\widehat{G}} m(\pi)\mathrm{Tr}\,(\pi(f)).$$

那么将这两种方法得到的 $\mathrm{Tr}\,(R(f))$ 的表达式相等便证明了 (在 $\Gamma\backslash G$ 为紧时的) Selberg 迹公式.

例如, 当 G 为交换群时, $\Gamma\backslash G$ 为紧, 且有正规化 $\mathrm{vol}\,(\Gamma\backslash G) = 1$, 则有 Selberg 迹公式

$$\sum_{\gamma\in\Gamma} f(\gamma) = \sum_{\pi\in\widehat{\Gamma\backslash G}} \pi(f),$$

于是由

$$\pi(f) = \int_G f(y)\pi(y)dy = \hat{f}(\pi^{-1})$$

(交换 π 与 π^{-1}), 最后便归结到 Poisson 求和公式

$$\sum_{\gamma\in\Gamma} f(\gamma) = \sum_{\pi\in\widehat{\Gamma\backslash G}} \hat{f}(\pi).$$

还有, 当 $\Gamma\backslash G$ 不是紧的时, 出现了 R 的不可约分解并非离散和等等问题, 然而就数论的 $G \supset \Gamma$ 等而言这些困难可由 Eisenstein 的一般性理论 (Selberg, Langlands) 等加以处理, 并得到了 Selberg 迹公式 (比较起 $\Gamma\backslash G$ 为紧的情形来, 在右端添加了补充项).

(b) Selberg 迹公式的第一个应用: Hecke 算子的迹公式

Selberg(1952 年左右) 将 Selberg 迹公式用到了 $G = SL_2(\mathbb{R}) \supset SL_2(\mathbb{Z}) = \Gamma$ (或

者 $G = SL_2(\mathbb{A}) \supset SL_2(\mathbb{Q}) = \Gamma$), 推导出了如下的 Hecke 算子的迹公式:

$$\begin{aligned}&\mathrm{Tr}(T(n)\,|\,S_k(SL_2(\mathbb{Z})))\\&= -\sum_{0\leqslant m<2\sqrt{n}}{}' \ H(4n-m^2)\frac{\eta_m^{k-1}-\bar{\eta}_m^{k-1}}{\eta_m-\bar{\eta}_m} - \sum_{\substack{d|n\\ d\leqslant\sqrt{n}}}{}' d^{k-1} + \frac{k-1}{12}\delta(\sqrt{n})n^{\frac{k}{2}-1}.\end{aligned}$$

这里的记号与 §11.1 相同. (Eichler(1956年) 给出了此公式的另一个代数几何式的证明.) 例如, 当 $k=12$ 时则成了公式

$$\tau(n) = \mathrm{Tr}\,(T(n)\,|\,S_{12}(SL_2(\mathbb{Z}))),$$

又由于在 $k \leqslant 10$ 以及 $k=14$ 有 $S_k(SL_2(\mathbb{Z})) = \{0\}$, 故

$$\mathrm{Tr}\,(T(n)\,|\,S_k(SL_2(\mathbb{Z}))) = 0,$$

因此 Selberg 公式给出了**类数关系式** (class number relations). 进一步容易看出 ($k \geqslant 4$ 为偶数)

$$\mathrm{Tr}\,(T(1)\,|\,S_k(SL_2(\mathbb{Z}))) = \dim S_k(SL_2(\mathbb{Z})) = \begin{cases}\left[\dfrac{k}{12}\right] & (k \not\equiv 2 \mod 12)\\[2ex] \left[\dfrac{k}{12}\right]-1 & (k \equiv 2 \mod 12).\end{cases}$$

Hecke 算子的迹公式可使用于

(A) 证明对于自守形式 f 与代数簇 X 的 $L(s,f) = L(s,X)$ (右端为 Hasse ζ),

(B) 证明对于自守形式 f_1, f_2 有 $L(s,f_1) = L(s,f_2)$,

等等对应于 Ramanujan Δ 的 Ramanujan 猜想, 可以按 (A) 那样做, 证明从 $L(s,\Delta)$ 的情形出发将其转换成 Hasse ζ 的性质（Weil 猜想）从而得到解决.

(c) Selberg 迹公式的第二个应用: Selberg ζ

考虑 Γ 为亏格 $g \geqslant 2$ 的紧 Riemann 面的基本群的情形. 此时有

$$M = \Gamma\backslash H = \Gamma\backslash SL_2(\mathbb{R})/SO(2),$$

并且

$$G = SL_2(\mathbb{R}) \supset \pi_1(M) = \Gamma$$

满足 (a) 小节所说的条件 (即 $\Gamma\backslash G$ 为紧), 从而 Selberg 迹公式成立.

Selberg 定义 Γ 的 **Selberg ζ** 为

$$\zeta_\Gamma^{\mathrm{Selberg}}(s) = \prod_{p\in\mathrm{Prim}\,(\Gamma)} (1-N(p)^{-s})^{-1}.$$

其中, Prim(Γ) 是 Γ 的素共轭类中所有素的那些 (不会变成其他共轭类的 2 次及以上的幂)的全体, $N(p)>1$ 取为 p 的特征值的绝对值的 2 次幂较大的那个. Selberg(1952 年左右) 利用 Selberg 迹公式证明了如下的结果:

(1) $\zeta_\Gamma^{\text{Selberg}}(s)$ 是可延拓为整个 s 平面的亚纯函数.

(2) 具有函数等式

$$\zeta_\Gamma^{\text{Selberg}}(s)\zeta_\Gamma^{\text{Selberg}}(-s)=(2\sin\pi s)^{4-4g}.$$

(3) $\zeta_\Gamma^{\text{Selberg}}(s)$ 的零点、极点的位置与阶可由全纯自守形式 $S_k(\Gamma)$ 的维数 (平凡的零点、极点) 以及实解析自守形式 $W_r^0(\Gamma)$ 的维数 (本质性的零点、极点) 决定. 这是按照 Laplace 算子的特征值对零点、极点的解释, 另外也得出了 $\zeta_\Gamma^{\text{Selberg}}(s)$ 的行列式表示 (参照 §9.5(c)) .

(4) $\zeta_\Gamma^{\text{Selberg}}(s)$ 满足类似的 Riemann 猜想 (虚的零点与极点全在 $\text{Re}(s)=\pm\frac{1}{2}$ 之上).

(5) $\zeta_\Gamma^{\text{Selberg}}(s)$ 在 $\text{Re}(s)\geqslant 1$ 上除去在 $s=1$ 的一阶极点外, 全纯没有零点, 由此事实知成立 "素共轭类定理"(素数定理的类比)

$$\pi_\Gamma(x)=\#\{p\in\text{Prim}(\Gamma)\mid N(p)\leqslant x\}\sim\frac{x}{\log x}.$$

这样的结果就连 $\Gamma=SL_2(\mathbb{Z})$ 等也已得证. 譬如, 在 $\Gamma=SL_2(\mathbb{Z})$ 时的 "素共轭定理" 为

$$\pi_{SL_2(\mathbb{Z})}(x)=\sum_{\varepsilon(d)^2\leqslant x}h(d)\sim\frac{x}{\log x},$$

从而解决了一个经典问题, 即关于判别式 $d>0$ 的不定二元二次型 (或者实二次域的整数环的子环) 的单位数 $\varepsilon(d)>1$ 与类数 $h(d)$ 的分布问题.

Selberg ζ 可以进行各种各样的推广. 数论的 ζ 与 Selberg 类型的 ζ 之间的关联因而也是一个研究课题.

§11.4 Langlands 猜想

所谓的**Langlands 猜想** (Langlands conjecture) 简单地说就是 " 所有 n 次好的 Euler 积全都是 GL_n 的自守 L 函数" 这样的猜想, 这是由 Langlands 在 20世纪60 年代末提出来的. 这里所说 "好的" 指的是, 它是可以解析延拓为整个 s 平面上的亚纯函数并具有 $s\leftrightarrow\alpha-s$ 这种类型的函数方程 (若正规化, 则设 $\alpha=1$ 即可). 这样的 Euler 积大体上可分为两类情形来考虑.

(A) 由 Galois 表示产生的 Euler 积.

(B) 由自守表示所产生的 Euler 积.

首先对于 (A) 我们设 K 为整体域, 这时对于所谓的 n 维连续表示

$$\rho: \mathrm{Gal}\,(\overline{K}/K) \to GL_n(\mathbb{C})$$
$$(\text{或者 } \rho: \mathrm{Gal}\,(\overline{K}/K) \to GL_n(\mathbb{Q}_l)),$$

构造如下的 n 次 Euler 积

$$L(s,\rho) = \prod_{v<\infty} \det(1-\rho(\mathrm{Frob}_v)N(v)^{-s})^{-1}$$

(v 遍历 K 的所有有限素点但忽略掉有限个 "坏素点"). 它被称为 Artin 类型的 L 函数. 这时的 **Langlands 猜想**是指 "存在 $GL_n(\mathbb{A}_K)$ 的自守表示 π, 使得 $L(s,\rho) = L(s,\pi)$ 成立" 这样的猜想. 当 $n=1$ 时, 我们已知利用类域论 (第八章定理 8.4) 的基本映射 $C_K \to \mathrm{Gal}\,(\overline{K}/K)^{ab}$ 可以构造出 $GL_1(\mathbb{A}_K)$ 的自守表示 π

$$\pi: C_K \to \mathrm{Gal}\,(\overline{K}/K)^{ab} \xrightarrow{\rho} \mathbb{C}^\times,$$

使得成立 $L(s,\rho) = L(s,\pi)$. 这意味着当 $n \geqslant 2$ 时, 可以称其为非交换类域论猜想.

容易理解的方面	Galois 方面
n 次自守表示 自守形式	$\mathrm{Gal}\,(\overline{K}/K)$的 n 维表示

这里, 当 $n \geqslant 2$ 时, 对 K 为正特征才可能 (而 $n=2$ 则完全能) 做到, 然而当 K 为数域时就不怎么了解了. 在数域的情形, 当 $\rho: \mathrm{Gal}\,(\overline{K}/K) \to GL_n(\mathbb{C})$ 时, 其像 $\mathrm{Im}\rho$ 在下面条件下的结果:

$n=2$: 如果 $\mathrm{Im}\rho$ 为可解群, 则 π 存在 (Langlands–Tunnell, 1981年),

$n \geqslant 3$: 如果 $\mathrm{Im}\rho$ 为幂零群, 则 π 存在 (Arthur–Clozel, 1989年).

它们每个的证明中 Selberg 迹公式都起了本质性的重要作用. 像将在第十二章叙述 $n=2$ 的 Langlands–Tunnell 的结果时所表明的那样, 它给出了 Wiles (1995年) 对 Fermat 猜想证明的关键.

至于 (B), 诸如在 §9.1(e) 出现的 $L(s,\mathrm{Sym}^m\Delta)$ 这个 $n=m+1$ 次 Euler 积, 以及在 §9.7(b) 出现的对于 m 次 Siegel 自守形式 f 的 $L(s,f)$ 这个 $n=2^m$ 次的 Euler 积都是这种例子. 在这些情形中都存在有 $GL_n(\mathbb{A})$ 的自守表示 π, 并猜想这些 Euler 积会与 $L(s,\pi)$ 一致. (作为应用的例子, 我们可得到, 如果对于 $m=1,2,3,\cdots$ 存在 $GL_{m+1}(\mathbb{A})$ 的自守表示 π_m 使得 $L(s,\mathrm{Sym}^m\Delta) = L(s,\pi_m)$, 则 Sato-Tate 猜想成立.)

得到解决的第一个非平凡的情形是对于 $L(s,\mathrm{Sym}^2\Delta)$ 构造了 $GL_3(\mathbb{A})$ 的自守表示 π_2, 并对于 $n=4$ 的情形 $L(s,\mathrm{Sym}^3\Delta)$ 以及 2 次的 Siegel 自守形式的 $L(s,f)$ 进行了完整的证明, 这是花了十来年才完成的课题.

对一般的情形请参看在本书末的参考文献中 [12] Bump 的书以及 [13] Bailey –Knapp 编纂的报告集 (都是 1997 年刊).

Langlands 猜想的证明方针在此可表述如下. 首先, 不管是在 (A), (B) 哪一个情形, 从已给的 n 次 Euler 积是能够构造 $GL_n(\mathbb{A}_K)$ 的表示 $\pi = \bigotimes_v \pi_v$ (假定已解决了局部 Langlands 猜想即可), 而问题在于 π 如何成为自守表示, 这时, 人们摸索出诸如

(1) 考察 $L(s,\pi)$ 的解析性质并使用逆定理,

(2) 寻找自守表示 π' 并根据 Selberg 迹公式 (与 Hecke 算子的迹公式比较; 参看 §11.3(b). 在那里的分类(A),(B)对应于这里的(A),(B)) 证明 $\pi \simeq \pi'$, 等等各种各样的方法.

小结

11.1 可以统一地将自守形式考虑为群上的函数. 相伴于它而出现的群的表示是自守表示. 对于自守表示也有 ζ 的理论.

11.2 研究自守表示之际, Selberg 迹公式起着积极的作用. Selberg 迹公式是 Poisson 求和公式到包含非交换群情形的推广, 它导出了 Selberg ζ 及 Hecke 算子的迹公式等等.

11.3 根据 Langlands 猜想, 期待有数论的 ζ 与 GL_n 自守表示的 ζ 的统一. 根据其部分结果证明了 Fermat 猜想. Langlands 猜想是类域论的推广, 也称其为非交换类域论猜想.

第十二章　椭圆曲线 (II)

本章讲述的是椭圆曲线的算术. 在 §12.1, 我们将解说谷山 (Taniyama)–志村 (Shimura)–Weil 关于椭圆曲线算术的猜想的含义是什么. 在 §12.2 则将极其粗略地叙述 Wiles 对 Fermat 猜想的证明思想. 由于篇幅的原因, 以及本书水准的限定, 本章的几乎所有的定理都没有给出证明. 希望有兴趣的读者能进一步走到卷末的参考文献所列举的书中去.

§12.1　有理数域上的椭圆曲线

(a) 有限域上的有理点

在此我们首先考虑具有有理系数的三次式. 譬如就取

$$y^2 = x^3 - x$$

吧. 对于这个不定方程的整数解、有理解以前已讲过了. 现在想要考虑的是比这些更简单的问题, 即当对此方程按素数 l 取 mod l 时, 对每个 l 数出它在 $\mathbb{F}_l = \mathbb{Z}/l$ 中解的个数. (这里之所以说是简单的, 其理由在于, 如果给出具体的素数, 则原则上其求解经有限次计算便能结束.)

我们来进行实际地求解.

$\mathbb{F}_2 = \mathbb{Z}/2$　　$(0,0),\ (1,0)$

$\mathbb{F}_3 = \mathbb{Z}/3$　　$(0,0),\ (1,0),\ (2,0)$

$\mathbb{F}_5 = \mathbb{Z}/5$　　$(0,0),\ (1,0),\ (2,1),\ (2,4),\ (3,2),\ (3,3),\ (4,0)$

$\mathbb{F}_7 = \mathbb{Z}/7$　　$(0,0),\ (1,0),\ (4,2),\ (4,5),\ (5,1),\ (5,6),\ (6,0)$

以下仅就解的个数列表看看.(表 12.1)

表 12.1

素数l	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67
解的个数	2	3	7	7	11	7	15	19	23	39	31	39	31	43	47	39	59	71	67

按 Fermat 还有 Gauss 的打算, 想要寻找出这种解的个数的规律.

问题 1 证明除 $l=2$ 外, 解的个数为除以 4 余 3 的数.

实际上成立以下定理.

定理 12.1 (Gauss) *设 l 为奇素数.*

(1) 当 $l=3 \pmod 4$ 时, 上述方程 $y^2=x^3-x$ 在 $\mathbb{F}_l$ 中解的个数为 l 个.

(2) 当 $l=1 \pmod 4$ 时, 如同在命题 0.2 中所说, 可写 l 为

$$l=a^2+b^2,\ a,b\in\mathbb{Z}.$$

在此设 a 为奇数, b 为偶数, 且进一步选取 a 的符号使得

$$当\ b\equiv 0 \pmod 4\ 时,\ a\equiv 1 \pmod 4)$$

$$当\ b\equiv 2 \pmod 4\ 时,\ a\equiv 3 \pmod 4.$$

这时, 上述方程 $y^2=x^3-x$ 在 $\mathbb{F}_l$ 中解的个数为 $l-2a$. □

我们在这里想要讲的是, 对于解的个数像在这里那样还是有规律可寻的. 即便在每个素数上解的个数是零乱的, 但还应该是分别可求的. 虽说如此, 也还是存在如此美妙的定理. 那么如此的理由是什么呢? 更一般的情形还成立吗?

现在稍稍考虑有一点不同的形式

$$y^2+y=x^3-x^2.$$

与前面一样地, 来进行解的计算, 得到

$$\begin{array}{ll}
\mathbb{F}_2=\mathbb{Z}/2 & (0,0),(0,1),(1,0),(1,1) \\
\mathbb{F}_3=\mathbb{Z}/3 & (0,0),(0,2),(1,0),(1,2) \\
\mathbb{F}_5=\mathbb{Z}/5 & (0,0),(0,4),(1,0),(1,4) \\
\mathbb{F}_7=\mathbb{Z}/7 & (0,0),(0,6),(1,0),(1,6),(4,2),(4,4),(5,1),(5,5),(6,3)
\end{array}$$

定理 12.2 (Eichler) *对于正整数 $n>0$, 设 a_n 是幂级数*

$$q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2=q-2q^2-q^3+2q^4+q^5+2q^6-2q^7+\cdots=\sum_{n=1}^{\infty}a_nq^n$$

展开的系数所决定的整数. 于是, 对于 $l\neq 11$, 上述方程 $y^2+y=x^3-x^2$ 在 $\mathbb{F}_l$ 中解的个数为 $l-a_l$. □

我们注意到 (§9.1(d)), 上面这个幂级数是权为 2 的 11 级自守形式. 还有, 当写出

$$q\prod_{n=1}^{\infty}(1-q^{4n})^2(1-q^{8n})^2=\sum_{n=1}^{\infty}b_nq^n$$

时, 可以证明 $y^2=x^3-x$ 在 $\mathbb{F}_l$ 中的解的个数为 $l-b_l$.

(b) 按 mod l 约化

在此, 我们将上面这类的方程考虑为椭圆曲线的方程, 那么, 按照对其系数取 mod l, 便可系统地考虑 $\mathbb{F}_l$ 上的曲线了.

当按照 mod l 对系数的约化 (reduction) 得到了 $\mathbb{F}_l$ 上的椭圆曲线 (即变为在 $\mathbb{F}_l$ 上的 $y^2=f(x)$, 其中 $f(x)$ 无重根) 时, 则称在 l 具**好约化**(good reduction), 如果不是这样则称为在 l 具**坏约化**(bad reduction). 例如, 对于 $y^2=x^3-x$, 有 $x^3-x=x(x-1)(x+1)$, 那么如果 $l\neq 2$, 则在 $\mathbb{F}_l$ 中$0,\pm1$ 互不相同, 故在奇素数具有好约化. 然而, 上述定义并不那么精确, 我们现在来好好地叙述它.

在第一章中, 我们称方程

$$y^2=ax^3+bx^2+cx+d\quad(a,b,c,d\in\mathbb{Q})$$

$$a\neq 0,\quad \text{右端无重根},$$

所代表的曲线为定义在有理数域上的椭圆曲线 (参看 §1.1(b)). 在这里由于我们所考虑的是按 mod l 对系数的约化, 所以必须再稍许精细地考虑一下. 譬如, 对 $y^2=27x^3-3x$ 作以 x 代替 $3x$ 的变换, 则变为 $y^2=x^3-x$. 就是说两者在 $\mathbb{Q}$ 上是同构的, 然而按其原样对前者取 mod 3 (即对系数取 mod 3) 则有 $y^2=0$, 这不是 $\mathbb{F}_3$ 上的椭圆曲线. 即便在同一条椭圆曲线上, 按照方程的取法不同则 mod l 约化的情形也不同, 这是使我们感到困惑的情形, 为此作如下考虑.

首先, 一般的整系数椭圆曲线 E 是指由三次式

$$E:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\ a_1,\cdots,a_6\in\mathbb{Z}\tag{12.1}$$

给出的曲线, 并满足下面的条件 (12.2). 令

$$b_2=a_1^2+4a_2$$
$$b_4=2a_4+a_1a_3$$
$$b_6=a_3^24a_6,$$

作在 $\mathbb{Q}$ 上将 y 换做 $\frac{1}{2}(y-a_1x-a_3)$ 的替换, 于是以上方程变为

$$y^2=4x^3+b_2x^2+2b_4x+b_6.$$

现令 $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$, 并定义

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

且称其为 E 的判别式. 当

$$\Delta \neq 0 \tag{12.2}$$

时, 则称 (12.1) 所给出的曲线 E 为整系数椭圆曲线.

现在, 取有理数 $u, r, s, t \in \mathbb{Q}$ $(u \neq 0)$, 以 $u^2x + r$ 替换 x, $u^3y + su^2x + t$ 替换 y, 便得到了新的 (12.1) 型的方程. (可以证明 $\mathbb{Q}$ 上同构的椭圆曲线可用此形变变为相同.) 新得到的方程可设为是整系数的. 在这样变形所得到的整系数的椭圆曲线之中其判别式绝对值最小的那个为**极小Weierstrass 模型** (minimal Weierstrass model).

例如, $y^2 = x^3 - x$ 与 $y^2 + y = x^3 - x^2$ 有共同的极小 Weierstrass 模型 (它们的判别式分别是 $32, -11$).

那么, 设 E 为定义在 $\mathbb{Q}$ 上的椭圆曲线. 按照上述的变形, 将 E 变为极小 Weierstrass 模型, 并计算出 b_i 和 Δ. 当素数 l 不除尽 Δ 时, 称 E 在 l 具**好约化**. 倘非如此, 则称 E 在 l 具**坏约化**. 当 E 在 l 为好约化时, (12.1) 的方程在其系数 $\bmod l$ 后变成 $\mathbb{F}_l$ 上的椭圆曲线. 具坏约化的素数只有有限个, 这是因为这种素数要除尽 Δ.

设 E 在 l 具坏约化. 当素数 l 不除尽 $b_2^2 - 24b_4$ 时, 称 E 在 l 具**乘法约化** (multiplicative reduction). 当 l 除尽 $b_2^2 - 24b_4$ 时, 则称 E 在 l 具**加法约化** (additive reduction). 好约化和乘法约化合并在一起被称为**半稳定约化** (semi-stable reduction). E 在所有素数均具半稳定约化 (即具好约化与乘法约化) 时, 则称 E 是一条**半稳定椭圆曲线** (semi-stable elliptic curve).

当 E 在 l 具乘法约化时, $E \bmod l$ 有奇点 (即当令 $f = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ 时, $\dfrac{\partial f}{\partial x} \bmod l$ 与 $\dfrac{\partial f}{\partial y} \bmod l$ 具有公共的零点). 让我们在 $\mathbb{F}_l$ 上考虑 E 的方程, 并形式地考虑切线之类的对象. 当在这个奇点的切线的斜率都属于 $\mathbb{F}_l$ 时, 称其为**分裂乘法约化**(split multiplicative reduction), 其他情形则称之为**非分裂乘法约化** (nonsplit multiplicative reduction).

例如, $y^2 = x^3 - x$ 在 $l = 2$ 具加法约化, 在除此之外的素数均具好约化. $y^2 + y = x^3 - x^2$ 在 11 以外为好约化, 而在 $l = 11$ 具分裂乘法约化.

(c) n 等分点与 Galois 群的作用

设 E 为定义在 $\mathbb{Q}$ 上的椭圆曲线. 对于椭圆曲线实数解全体构成的图像已在第一章描述过了, 而其复数解全体构成图像 (准确地说这是个 Riemann 面) 形成一个环面 (具有一个空洞的环面). 这时, 上述方程在复数域上可变形为

$$y^2 = 4x^3 - g_2x - g_3,$$

从而成立以下定理.

定理 12.3 对于椭圆曲线 $E: y^2 = 4x^3 - g_2x - g_3$, 存在 $\mathbb{R}$ 上线性独立的复数 ω_1, ω_2 满足以下条件.

(i)

$$g_2 = 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(m\omega_1 + n\omega_2)^4}, \quad g_3 = 140 \sum_{(m,n)\neq(0,0)} \frac{1}{(m\omega_1 + n\omega_2)^6},$$

其中 (m, n) 遍历除去 $(0,0)$ 以外的所有整数组.

(ii) 进一步, 令

$$\wp(z) = \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right),$$

并令 $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, 则有群的同构映射

$$\mathbb{C}/L \xrightarrow{\simeq} E(\mathbb{C})$$

$$z \mapsto (\wp(z), \wp'(z)).$$

这里的 $E(\mathbb{C})$ 是 E 的所有 $\mathbb{C}$ 有理点全体构成的 Abel 群 (参看 §1.2(a)). □

从拓扑上说, $\mathbb{C}/L$ 与环面同胚. 设 $n > 0$ 为正整数时, 在群 $\mathbb{C}/L$ 中被 n 倍消去的所有元全体 $E[n] = \{x \in \mathbb{C}/L \mid nx = 0\}$ 同构于 $\mathbb{Z}/n \oplus \mathbb{Z}/n$:

$$E[n] = \{x \in \mathbb{C}/L \mid nx = 0\} \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

另外, 设 $P = (x, y) \in E(\mathbb{C})$, $nP = 0$, 则可以证明 P 的坐标 x, y 都在 $\mathbb{Q}$ 上是代数的.

以 $\overline{\mathbb{Q}}$ 表示有理数域 $\mathbb{Q}$ 的代数闭包, 记其 Galois 群为 $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. 对于上面那样的 $P = (x, y)$ 定义 Galois 群的元 $\sigma \in G_{\mathbb{Q}}$ 的作用为 $\sigma(P) = (\sigma(x), \sigma(y))$. 对应于上面的同构存在基底 e_1, e_2, 使得对 $P \in E[n]$ 的 P 可表示为

$$P = ae_1 + be_2,\ a, b \in \mathbb{Z}/n.$$

如果 $nP = 0$, 那么由于 $n\sigma(P) = \sigma(nP) = 0$, 故 $\sigma(P)$ 也属于 $E[n]$. 于是如果令

$$\sigma(e_1) = ae_1 + ce_2,\ \sigma(e_2) = be_1 + de_2,$$

那么 σ 在 n 倍消去的点上的作用则可用矩阵

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/n)$$

表出. 这样一来便定义了群的同态映射

$$G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/n)$$

$$\sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

我们把以上所说集中成定理 12.4 (1). 而上面的同态映射则满足性质 (2).

定理 12.4

(1) 设 E 为定义在 $\mathbb{Q}$ 上的椭圆曲线, $E[n]$ 为 $E(\mathbb{C})$ 中所有 n 倍消去的元构成的子群. 此时, 作为 Abel 群的 $E[n]$ 同构于 $\mathbb{Z}/n \oplus \mathbb{Z}/n$. $E[n]$ 中元的坐标在 $\mathbb{Q}$ 上是代数的, 因而 $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 可作用其上. 按照这个作用定义了同态映射

$$\rho_{E[n]} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/n).$$

(2) 设 $K_n/\mathbb{Q}$ 为上面的同态映射的核 $\mathrm{Ker}\rho_{E[n]}$ 所对应的扩域. 这就是说, 设有 $\mathrm{Gal}(K_n/\mathbb{Q}) = \mathrm{Ker}\rho_{E[n]}$. 设 l 为素数, 且 E 在 l 具好约化, 另外 l 还与 n 互素. 此时, l 在 $K_n/\mathbb{Q}$ 中非分歧. □

(d) Tate 模

设 E 如上, p 为素数. 对于正整数 n, 考虑 p^n 等分点 $E[p^n]$, 并称其关于 p 倍映射 $p : E[p^{n+1}] \to E[p^n]$ 的逆极限

$$T_p(E) = \varprojlim E[p^n]$$

为 **Tate 模** (Tate module). $T_p[E]$ 为秩 2 的自由 $\mathbb{Z}_p$ 模. Galois 群 $G_{\mathbb{Q}}$ 作用于 $T_p[E]$ 上. 设 e_1, e_2 为 $T_p[E]$ 作为 $\mathbb{Z}_p$ 模的基底, 并设

$$\sigma(e_1) = ae_1 + ce_2, \quad \sigma(e_2) = be_1 + de_2,$$

则定义

$$\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_p),$$

从而得到了连续映射

$$\rho_p : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p).$$

这个同态映射也可以作为作用于 $E[p^n]$ 上的 $\rho_{E[p^n]} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/p^n)$ 的逆极限来把握.

此时, 有限域上的方程解的个数与这个 Galois 群的作用之间成立以下关系.

定理 12.5　设 $K_{p^\infty}/\mathbb{Q}$ 为对应于上面的同态映射

$$\rho_p : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p)$$

的核 $\mathrm{Ker}\rho_p$ 的扩域. 也就是说, 设 $\mathrm{Gal}(\overline{\mathbb{Q}}/K_{p^\infty}) = \mathrm{Ker}\rho_p$. 设 l 为素数, 且 E 在 l 具好约化, 又设 $l \neq p$. 则此时 l 在 $K_{p^\infty}/\mathbb{Q}$ 非分歧, 若设 Frob_l 为在 l 的 Frobenius 共轭类, 则成立

$$\det(\rho_p(\mathrm{Frob}_l)) = l$$

(因此, $\det(\rho_p)$ 与分圆特征 κ (§10.1(e)) 一致). 另外, 若令

$$\mathrm{Tr}\,(\rho_p(\mathrm{Frob}_l)) = a_l,$$

则 a_l 为整数, 且成立

$$\#E(\mathbb{F}_l) = l + 1 - a_l.$$

这里的 $E(\mathbb{F}_l)$ 为 E 的全体 $\mathbb{F}_l$ 有理点 (即方程在 $\mathbb{F}_l$ 中的解与原点形成的群), 于是 $\#E(\mathbb{F}_l)$ 为 "方程解的个数"+1. □

如此一来, 方程解的个数可以从 Galois 群的作用得到, 这是个使人惊讶的事. 还有, 上面的定理还说明以上的 $\mathrm{Tr}\,(\rho_p(\mathrm{Frob}_l))$ (即 a_l) 不依赖于 p. 因此, 就椭圆曲线 E 而言, 知道存在着具有非常重要意义的数列 $(a_l)_l$(这里的 l 遍历所有具好约化的素数).

(e) 椭圆曲线的 ζ 函数及 L 函数

关于 $\mathbb{Z}$ 上有限生成环的 Hasse ζ 函数已在 §7.4 中讲过. 对于 $\mathbb{Z}$ 上的有限型概形 (scheme) 也可以同样地定义 Hasse ζ 函数.

对于 $\mathbb{Q}$ 上的椭圆曲线 E, 在 $\mathbb{Z}$ 上取的一个适当的模型, 则可定义 Hasse ζ 函数如下.

$$\zeta_E(s) = \prod_{l:\text{好约化}} \frac{1 - a_l l^{-s} + l^{1-2s}}{(1-l^{1-s})(1-l^{-s})} \prod_{l:\text{分裂乘约化}} \frac{1}{1-l^{1-s}}$$
$$\times \prod_{l:\text{非分裂乘约化}} \frac{1+l^{-s}}{(1-l^{1-s})(1-l^{-s})} \prod_{l:\text{加约化}} \frac{1}{(1-l^{1-s})(1-l^{-s})}$$

在这里, 上面的第一个积遍历所有具好约化的素数, 第二、第三、第四个积分别遍历分裂乘约化的、非分裂乘约化的、加法约化的素数. 第一个积中的 a_l 为 $a_l = l + 1 - \#E(\mathbb{F}_l)$. 由于具坏约化的素数只有有限个, 故主要的项是第一个积. 请注意, 在 E 的 ζ 函数这样的重要函数中, 再一次出现了 (a_l) 这个数列.

E 的 L 函数的定义如下.

$$L(E,s) = \prod_{l:\text{好约化}} \frac{1}{1 - a_l l^{-s} + l^{1-2s}} \times [\text{具坏约化的素数的贡献}]$$

$$[\text{具坏约化的素数的贡献}] = \prod_{l:\text{分裂乘约化}} \frac{1}{1-l^{-s}} \prod_{l:\text{非分裂乘约化}} \frac{1}{1+l^{-s}},$$

由上面可知有

$$\zeta_E(s) = \zeta_{\mathbb{Z}}(s)\zeta_{\mathbb{Z}}(s-1)L(E,s)^{-1}.$$

此处的 $\zeta_{\mathbb{Z}}(s)$ 为 Riemann ζ 函数. 将 $L(E,s)$ 考虑为 $\zeta_E(s)$ 的主要部分就可以了. 我们已知 $L(E,s)$ 在 $\mathrm{Re}\,(s) > 3/2$ 中绝对收敛. 有猜想说 $L(E,s)$ 可全纯地解析延拓到全平面 $\mathbb{C}$, 此后将陈述的 Wiles 定理解决了在半稳定的情形, 之后 Wiles 的方法得到了进一步发展从而现在已完全得到解决.

对于椭圆曲线 E 而言, L 函数 $L(E,s)$ 是非常重要的函数. 譬如有 **Birch–Swinnerton–Dyer 猜想**这样有名的未解决问题. 在此我们不打算给予完整的叙述, 但叙述其中关于 Mordell–Weil 群 $E(\mathbb{Q})$ 作为 Abel 群的秩 (rank) 的猜想. Birch 和 Swinnerton–Dyer 猜测成立

$$\mathrm{order}_{s=1} L(E,s) = \mathrm{rank} E(\mathbb{Q}).$$

也就是说, Mordell–Weil 群的秩这个在数论上非常重要的量可以通过 L 函数的信息得到了解. 关于这个猜想, 在左端为 0 或 1 时, 由于最近的惊人进步, 已能够相当了解了, 而在左端大于等于 2 时, 则完全没有解决.

还有, 当 K 为数域时, 我们回忆关于 $\zeta_K(s)$ 在 $s=0$ 的阶有

$$\begin{aligned}\mathrm{order}_{s=0}\zeta_K(s) &= r_1 + r_2 - 1\\ &= \mathrm{rank}\, O_K^{\times} \quad (O_K^{\times}\text{为 } K \text{ 的单位群})\end{aligned}$$

(参看定理 7.10). Birch–Swinnerton–Dyer 猜想是它的一个类比.

现在把说过的东西小结一下. 对于定义在有理数域上的椭圆曲线 E, 以 $\mathcal{L}$ 表示具有好约化的素数全体的集合. 这时, 可定义整数数列 $(a_l)_{l\in\mathcal{L}}$, 这些数 a_l 出现在一些非常重要的场合.

(1) 设 $\mathbb{F}_l$ 是 l 个元构成的有限域, 则关于 $\mathbb{F}_l$ 有理点的个数成立

$$a_l = l + 1 - \#E(\mathbb{F}_l)$$

(将此想成是 a_l 的定义也行).

(2) 根据 Galois 群 $G_{\mathbb{Q}}$ 在 Tate 模 $T_p(E)$ 上的作用, 可定义连续同态映射

$$\rho_p : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p),$$

如果有 $l \neq p$, 则成立

$$a_l = \mathrm{Tr}\,(\rho_p(\mathrm{Frob}_l)).$$

(3) $(a_l)_{l\in\mathcal{L}}$ 出现在 E 的 ζ 函数以及 L 函数的 Euler 积之中.

(f) 模椭圆曲线

为了研究椭圆曲线的算术, 了解 $(a_l)_{l\in\mathcal{L}}$ 这个数列是极其重要的, 这一点我们在前小节为止已经讲到了. 但感到吃惊的是, 这些数 a_l 竟然与自守形式有关联.

猜想 12.6 (谷山–志村–Weil) 设 E 为定义在 $\mathbb{Q}$ 上的椭圆函数, $\mathcal{L}$ 为那些素数的集合, 使得 E 在这些素数上具好约化, 而 $(a_l)_{l\in\mathcal{L}}$ 如上所定义. 此时存在按 q 展开而 q^l 的系数为 a_l 的自守形式 $\sum a_n q^n$.

再详细一点说就是, 对于 $\mathbb{Q}$ 上定义的椭圆曲线 E, 如果能定义被称做导子的正整数 N, 则存在 q^l 的系数为 a_l 的、权 2 的、N 级 ($\Gamma_0(N)$ 级) 的 Hecke 算子的同时特征函数 $\sum a_n q^n$ □

定理 12.2 表明这个猜想对于椭圆曲线 $y^2+y=x^3-x^2$ 是正确的. 另外像 (a) 小节最后面指出过的那样, $y^2=x^3-x$ 也有对应的自守形式.

谷山在 1955 年作为问题陈述了这个猜想的原始形式. 而后志村在 20世纪60 年代对于其给出了上面形式严格的公式化阐述. 再以后, 由于 Weil 的研究 (1967年), 使得这个猜想广为人知.

一般地, 对于作为权 2、N 级的、Hecke 算子的同时特征函数的尖点形式 $f=\sum a_n q^n\,(a_1=1)$, 若令 $K=\mathbb{Q}_p(\{a_n|n\geqslant 2\})$, Eichler 和志村证明了 $K/\mathbb{Q}_p$ 为有限扩域, 且存在不可约连续表示

$$\rho_f: G_{\mathbb{Q}}=\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to GL_2(K)$$

满足 $\mathrm{Tr}\,(\rho_f(\mathrm{Frob}_l))=a_l$, $\det(\rho_f(\mathrm{Frob}_l))=l$. 这个表示是对模曲线 (modular curve) $X_0(N)$ 的 Jacobi 簇 $J_0(N)$ 的 Tate 模按照 Hecke 算子进行分解时, 由 $G_{\mathbb{Q}}$ 对于 f 分量的作用得到的.

现在设 $f=\sum a_n q^n$ 为权 2 的、N 级的 Hecke 算子的同时特征函数的尖点形式, 并设其系数 a_n 都是有理数 (并取 $a_1=1$). 于是, 将模曲线 $X_0(N)$ 的 Jacobi 簇 $J_0(N)$ 按照 Hecke 算子分解时其 f 分量为一维 Abel 簇, 也就是说是条椭圆曲线, 记此椭圆曲线为 E, 我们有

$$\mathrm{Tr}\,(\rho_f(\mathrm{Frob}_l))=\mathrm{Tr}\,(\rho_E(\mathrm{Frob}_l))=a_l.$$

因此, 这条椭圆曲线 E 满足了猜想 12.6 的条件.

称这样得到的椭圆曲线 (和同源的椭圆曲线) 为**模椭圆曲线**. (若使用 Faltings 所证明的一般性的同源定理进行叙述的话) 谷山–志村–Weil 猜想所叙述的便是, 所有 $\mathbb{Q}$ 上定义的椭圆曲线均是模椭圆曲线. 自守形式的世界是个具有非常多对称性的美丽世界. 所有的椭圆曲线都来自这个世界, 乍一看这似乎是个令人吃惊的猜想. 然而, 譬如对于模椭圆曲线, 已知其 L 函数可解析延拓 (在 (e) 小节中叙述过的 Hasse 猜想) 到全平面 (参看定理 9.7). 此外, 反过来 Weil 也证明了 (1967年), 在 $\mathbb{Q}$ 上定义的椭圆曲线 E 的 L 函数 $L(E,s)$ 被解析延拓到整个 $\mathbb{C}$, 如果满足某个函数方程, 则 E 是模的. 据此, 猜想 12.6 被看成是绝对正确的.

设 $L(E,s)$ 为定义在 $\mathbb{Q}$ 上的椭圆曲线 E 的 L 函数. $L(E,s)$ 像在 (e) 小节中那

样由 Euler 积定义, 形式地可写为 Dirichlet 级数的样子:

$$L(E,s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}.$$

右端的 a_n 与 L 函数的 Euler 积定义中的 a_l (即上面一直在说的那些 a_l) 一致. 此时, 谷山–志村–Weil 猜想可改写为以下形式.

猜想 12.6′ (谷山–志村–Weil) 设 E 为定义在 $\mathbb{Q}$ 上的导子为 N 的椭圆曲线, 而

$$L(E,s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

为其 L 函数. 则此时

$$f=\sum_{n=1}^{\infty}a_nq^n$$

为权 2 的 N 级自守形式. □

上面是换成使用 ζ 函数的说法, 还可换成一种代数几何的说法. 像上面那样, 这个说法是, $\mathbb{Q}$ 上定义的任意椭圆曲线均出现在模曲线的 Jacobi 簇的分量上 (准确地说, 同源于 Jacobi 簇的分量).

这是下面猜想的另一种说法.

猜想 12.6″ (谷山–志村–Weil) 设 E 为定义在 $\mathbb{Q}$ 上的导子为 N 的椭圆曲线, 存在从模曲线到 E 的非零态射 (morphism)

$$X_0(N)\to E$$ □

也就是说, E 被 $X_0(N)$ 所参数化 (parametrize). 将它与所有二次域包含在分圆域的 Gauss 定理 (命题 5.13) 相比较是有意思的. 椭圆曲线是射影直线的二次覆叠. 可是, 谷山–志村–Weil 猜想说的是它必定能按照模曲线参数化. 如此考虑的话, 谷山–志村–Weil 猜想则可看成为 Gauss 定理的代数几何版.

从 Galois 群的表示来看谷山–志村–Weil 猜想将在 §12.2(c) 讲述.

§12.2 Fermat 猜想

(a) Frey 曲线

终于到了可以讲述关于 Fermat 猜想的时候了. 先做点准备, 考虑以下这样的椭圆曲线. 设 A,B,C 为满足

$$A+B=C$$
$$A\equiv 3 \pmod 4),\ B\equiv 0 \pmod{32}$$

的互素的整数. 这时, 考虑椭圆曲线

$$E: y^2 = x(x-B)(x-C).$$

作置换 $x = 4X$, $y = 8Y + 4X$, 则上式成为

$$Y^2 + XY = X^3 - \frac{B+C+1}{4}X^2 + \frac{BC}{16}X.$$

这是 E 的极小 Weierstrass 模型. 按照定义计算 E 的判别式 Δ, 得到

$$\Delta = \frac{(ABC)^2}{2^8}.$$

在除尽 Δ 的素数处, E 为乘法约化. 特别地, E 为半稳定椭圆曲线 (关于其定义, 请见 §12.1(b)).

设 p 为奇素数, 考虑由 E 的 p 等分点 $E[p]$ 产生的表示

$$\rho_{E[p]}: G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/p).$$

像定理 12.4 那样, 我们记对应于这个同态映射的核 $\mathrm{Ker}\rho_{E[p]}$ 的域为 K_p. 考虑

$$\det(\rho_{E[p]}): G_{\mathbb{Q}} \to (\mathbb{Z}/p)^\times$$

$$\sigma \mapsto \det(\rho_p(\sigma)),$$

于是根据定理 12.4, 因为有 $\det(\mathrm{Frob}_l) = l$, 故知 $\det(\rho)$ 不是别的, 正是 Teichmüller 特征 ω (§10.1(e)). 就是说, 当设 μ_p 为 $\overline{\mathbb{Q}}$ 中所有 p 次单位根构成的群时, 它是对于任意的 $\zeta \in \mu_p$, 使得 $\sigma(\zeta) = \zeta^{\omega(\sigma)}$ 成立的特征. 特别地, 我们注意到有 $\mathbb{Q}(\mu_p) \subset K_p$.

定理 12.7 设 l 为奇素数,

(i) 设 l 不除尽 ABC, 且不同于 p, 则 l 在 K_p 中非分歧.

(ii) 设 l 除尽 ABC, 且 $l \neq p$. 于是有以下等价

$$l \text{ 在 } K_p \text{ 中非分歧} \iff \mathrm{ord}_l(ABC) \equiv 0 \pmod{p}.$$

(iii) 如果 $\mathrm{ord}_p(ABC) \equiv 0 \pmod{p}$, 则 p 在 K_p 中 "小分歧". 这里, 在现在的情形, 所谓 p 为 "小分歧" 是指成立如下的断言. 设 v 为 p 之上在 K_p 中的素理想时, K_p 在 v 处的完备化 $(K_p)_v$ 可写为

$$(K_p)_v = k(\mu_p)(\sqrt[p]{u}), \quad u \in O_{k(\mu_p)}^\times,$$

其中 k 为 $\mathbb{Q}_p$ 的有限非分歧扩域. □

设 π 是 $O_{K(\mu_p)}$ 的极大理想的生成元, 考虑扩张 $k(\mu_p)(\sqrt[p]{\pi})/k$, 这一扩张的判别式的赋值比这定理中扩张的判别式的赋值要大, 上面所说的 "小分歧" 从此而来.

要证明定理 12.7 必须要有 Tate 曲线的理论.

G. Frey 发现了 Fermat 猜想与下面要讲的椭圆曲线的算术有关. 设 p 为大于等于 5 的素数, 并设存在正整数 a, b, c 满足

$$a^p + b^p = c^p.$$

不妨设 a 为奇数, b 为偶数. 当 $a \equiv 3 \pmod 4$ 时, 令 $A = a^p, B = b^p, C = c^p$, 而当 $a \equiv 1 \pmod 4$ 时, 则令 $A = -c^p, B = b^p, C = -a^p$. 考虑椭圆曲线

$$E_{(a,b,c)} : y^2 = x(x-B)(x-C).$$

称此椭圆曲线为**Frey 曲线 (Frey curve)**. Frey 证明了 (1986 年) 这样曲线的存在与 Serre 的 ϵ 猜想以及谷山–志村–Weil 猜想相违背. 也就是说, 从这两个猜想就可以推导出 Fermat 猜想. 按照这个事实, Fermat 猜想才被认为是一个真实可信的猜想类型了. 在此之后, 由于 Ribet 证明了 Serre 的 ϵ 猜想 (1989 年), 于是 Fermat 定理便转化成了可由谷山–志村–Weil 猜想推出的事了. 在下面的 (b) 小节中我们将叙述 Ribet 的定理.

(b) Ribet 定理

设 $f = \sum a_n q^n$ 为权 $k \geqslant 2$ 的 N 级的 Hecke 算子的同时特征函数的尖点形式. 令 $K = \mathbb{Q}_p(\{a_n | n \geqslant 2\})$, 于是 $K/\mathbb{Q}_p$ 为有限扩域, 且存在连续不可约表示

$$\rho_f : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(K),$$

其满足 $\mathrm{Tr}(\rho_f(\mathrm{Frob}_l)) = a_l$, $\det(\rho_f(\mathrm{Frob}_l)) = l^{k-1}$. 这个事实在 $k=2$ 时, 如 §12.1(f) 所说, 由 Eichler、志村证明, 而一般情形则由 Deligne 所证明.

设 O_K 为 K 的整数环, 由于 $G_{\mathbb{Q}}$ 为紧, 故 ρ_f 的像可取在 $GL_2(O_K)$ 之中. 又设 π 为 O_K 的极大理想的生成元, $\mathbb{F}$ 为其剩余域, 并考虑

$$\rho_f \mod \pi : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}).$$

按照定义, 由于

$$\mathrm{Tr}(\rho_f \mod \pi(\mathrm{Frob}_l)) = a_l \mod \pi, \quad \det(\rho_f \mod \pi(\mathrm{Frob}_l)) = l^{k-1} \mod \pi,$$

如果 $\rho_f \mod \pi$ 是不可约的, 那么 $\rho_f \mod \pi$ (的同构类) 由 f 唯一地决定. 如此所得到的有限域 $\mathbb{F}$ 上的二维表示被称做权 k 的 N 级模表示.

Serre 猜测, 对于任意有限域 $\mathbb{F}$, 满足 $\det \rho_0(c) = -1$ (c 为复共轭) 的绝对不可约表示 $\rho_0 : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ 全都是模表示. 并且, 也猜测此时的权 k 与级 N 应该怎么由 ρ_0 决定 (**Serre 猜想**). Ribet 继 Mazur 之后解决了 Serre 猜想中被称做 ϵ 猜想的部分.

定理 12.8 (Mazur, Ribet) 设 $\mathbb{F}$ 为特征 $p \geqslant 5$ 的有限域. 又设不可约表示 $\rho_0 : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ 为权 2 的 N 级的不可约模表示, 并且 N 不含有平方因子. 另外, 设 K_{ρ_0} 为 ρ_0 的核所对应的域, 而 l 为除尽 N 的奇素数. 于是

(i) 设 $l \neq p$, 且 l 在 K_{ρ_0} 上非分歧, 于是 ρ_0 为权 2 的 N/l 级的模表示.

(ii) 设 p 除尽 N, 且 p 在 K_{ρ_0} 上为 "小分歧", 于是 ρ_0 为权 2 的 N/p 级的模表示. □

设 p 为不小于 5 的素数, 假定 Fermat 猜想不成立, 从而

$$a^p + b^p = c^p$$

存在整数解. 考虑在 (a) 小节所说的 Frey 曲线 $E = E_{(a,b,c)}$, 并假定对于 E 谷山–志村–Weil 猜想为真.

将这个定理应用于由 E 的 p 等分点所产生的表示 $\rho_{E[p]}$ 来看看. 首先, 我们知道这个表示是不可约的 (为此, 应用 Mazur 的定理, 即定义在 $\mathbb{Q}$ 上的椭圆曲线的全部等分点构成的群的阶不大于 16). 那么, 因为由假定 $E = E_{(a,b,c)}$ 为模椭圆曲线, 故得知 $\rho_{E[p]}$ 为权 2 级 $N = \prod_{l|\Delta} l$ 的模表示. 于是, 由定理 12.7 和定理 12.8, $\rho_{E[p]}$ 成为了权 2 级 2 模表示. 然而, 不存在权 2 级 2 的尖点形式. 这引出了矛盾. 因此, 最初的假定, 即 a, b, c 的存在是错误的, 从而证明了 Fermat 定理.

按照上面这样, 为了证明 Fermat 猜想, 只要能说 $E_{(a,b,c)}$ 是模曲线就可以了. 回忆一下: $E_{(a,b,c)}$ 是条半稳定椭圆曲线. 对此, Wiles 证明了下面的定理 (1995 年).

定理 12.9 (Wiles) 定义在 $\mathbb{Q}$ 上的半稳定椭圆曲线为模曲线. □

从而有

推论 12.10 (Fermat 猜想) 对大于等于 3 的整数 n, 不存在满足

$$a^n + b^n = c^n$$

的正整数 a, b, c. □

推论 12.10 中的 $n = 3$, $n = 4$ 的情形由 Euler(或许也由 Fermat 自己) 证明, 故只要设素数 p 不小于 5 就可以了. 故由上述讨论得出了推论 12.10.

下面我们来叙述定理 12.9 的证明思路.

(c) 模 Galois 表示的提升

设 O 为局部域的整数环. 当 $G_{\mathbb{Q}}$ 的表示 $\rho : G_{\mathbb{Q}} \to GL_2(O)$ 相伴于自守形式 f 的表示时 (即对应的 $G_{\mathbb{Q}}$ 模为同构时), 则说 ρ 是由自守形式得来的. 此时, 由迄今所叙述过的事实 (并使用 Faltings 的同源定理), 得知下面的定理成立.

定理 12.11 设 E 为定义在 $\mathbb{Q}$ 上的椭圆曲线, 此时下面的两个论断等价.

(1) E 为模曲线.

(2) 存在某个素数 p, 使得由 Tate 模 $T_p(E)$ 产生的表示 ρ_p 是从自守形式得来的. □

这是谷山–志村–Weil 猜想 (猜想 12.6) 换成 Galois 表示的说法.

由定理 12.11 知, 为了断言一条椭圆曲线为模的, 只要对一个素数 p 能断言 ρ_p 是由自守形式得来的就可以了. 为了证明定理 12.9, Wiles 主要使用了 $p = 3$. 如此说是由于, 当 $\rho_{E[3]}$ 为不可约时, 因为按照 Langlands 和 Tunnell 所断言, $\rho_{E[3]}$ 是模表示 (参看 §11.4), 从而存在推断的基础.

Wiles 所证明的是下述定理. 设 p 为奇素数.

定理 12.12 (Wiles) 设 $\mathbb{F}$ 为特征 p 的有限域,

$$\rho_0 : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$$

为模表示, 并设满足以下条件.

(1) 将 ρ_0 限制在 $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}))$ 上时为绝对不可约.

(2) $\det(\rho_0) = \omega$ (ω 为 Teichmüller 特征).

(3) 将 ρ_0 限制在分解群上时的条件 (我们对其在此略去. 限制于在 p 的分解群时的条件是特别重要的. E 为半稳定椭圆曲线时, $\rho_{E[p]}$ 满足这个条件).

设 O 为局部域的整数环, π 为其极大理想的生成元, 而

$$\rho : G_{\mathbb{Q}} \to GL_2(O)$$

为使 $\rho \bmod \pi = \rho_0$ 成立的表示. 进一步设 ρ 还满足下面的 (i),(ii),(iii).

(i) 设 K_ρ 为对应于 ρ 的核的域, 则在 $K_\rho/\mathbb{Q}$ 上分歧的素数为有限个.

(ii) $\det(\rho) = \kappa$ (κ: 分圆特征).

(iii) 将 ρ 限制在分解群上时的条件 (对其在此略去. 当 E 为半稳定椭圆曲线时, 由 Tate 模产生的表示满足此条件).

于是在此时, ρ 是由自守形式得来的. □

虽然 Wiles 处理了更一般情形的 $\det(\rho)$, 但上面所说的情形对定理 12.9 的证明所必需的材料是足够的了.

根据刚才所说的, 成为不可约表示的

$$G_{\mathbb{Q}} \to GL_2(\mathbb{F}_3)$$

是模表示这个事实是由 Langlands 和 Tunnell 证明的 (1981 年). 在这个证明中, 实质性地使用了 $GL_2(\mathbb{F}_3)$ 为可解群的事实. 因此对于 $GL_2(\mathbb{F}_p)$ ($p \geqslant 5$) 不适合应用这个方法.

根据定理 12.12, 定理 12.11, 首先知道了如下事实.

“设 E 为半稳定椭圆曲线, 并设由 3 等分点产生的表示 $\rho_{E[3]}$ 在 $\mathbb{Q}(\sqrt{-3})$ 的绝对 Galois 群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ 上的限制也是绝对不可约的, 那么在这个条件下, E 为模椭圆曲线.”

Wiles 巧妙地借助于使用 5 等分点证明了也可以去掉上面那个不可约条件 (关于其技术方面在这里也不可能讲述), 于是最后成功地证明了所有的半稳定椭圆曲线为模曲线.

(d) $R = T$

由于定理 12.12 为 Wiles 的 Fermat 猜想证明中最重要的定理, 在下面我们将给出这个定理证明的概述. 定理 12.12 断言满足所给条件的表示全是由自守形式得来的, 从而我们注意到它与 Mazur 和 Wiles 对岩泽主猜想证明方法 (§10.3(e))“所有非分歧扩张均由自守形式得出” 的类似性. 在证明中, Mazur 的 Galois 表示的形变理论起了本质的作用.

让 ρ_0 如定理 12.12 中所设. 此时, 对于满足定理 12.12 的 (i), (ii), (iii) 的这些 ρ, 存在满足以下那样性质的环 R 及 Galois 表示

$$\rho_R : G_{\mathbb{Q}} \to GL_2(R).$$

若有满足定理 12.12 的条件 (i), (ii), (iii) 的 ρ, 则存在环同构

$$R \to O,$$

并且由这个环同态产生的同态映射 $GL_2(R) \to GL_2(O)$ 与 ρ_R 的复合

$$G_{\mathbb{Q}} \overset{\rho_R}{\to} GL_2(R) \to GL_2(O)$$

与 ρ 等价. 另一方面, 即便添加条件 “ρ 由自守形式得出来” 到 (i), (ii), (iii) 中, 也存在一般的环 T 和 Galois 表示

$$\rho_T : G_{\mathbb{Q}} \to GL_2(T),$$

且满足这样的条件的模表示 ρ 均由 ρ_T 得到. 这就是说, 如果设有这样的 ρ, 则存在那样的环同态映射 $T \to O$, 使得这个环同态产生的同态映射 $GL_2(T) \to GL_2(O)$ 与 ρ_T 的复合

$$G_{\mathbb{Q}} \overset{\rho_T}{\to} GL_2(T) \to GL_2(O)$$

与 ρ 等价. T 是由 Hecke 环 (由 Hecke 算子产生的环) 构造出的. 使用这样的形变理论的语言的话, 定理 12.12 只需简单地表示为

$$R = T.$$

由 R 与 T 的定义, 我们有环同态映射

$$R \to T,$$

并可证明它为满射. 我们的目的是要证明这个映射是个同构.

下面的定理为 H.W. Lenstra Jr. 通过改进 Wiles 的方法所证明的, 因为比起 Wiles 原本的定理它的叙述要容易些, 我们叙述于此.

定理 12.13 (Lenstra Jr.) *设 O 为局部域的整数环, R 为 O 上的完备 Noether 局部环, T 为 O 上的有限平坦 (finite flat) 的 Noether 局部环. 假定有满的 O 线性环同态映射 $\varphi: R \to T$, $\psi: T \to O$, 并令 $\phi = \psi \circ \varphi$. 设 $\mathrm{Ann}_T(\mathrm{Ker}\psi)$ 为 $\mathrm{Ker}\psi$ 的零化子. 此时, 如果*

$$\#((\mathrm{Ker}\phi)/(\mathrm{Ker}\phi)^2) \leqslant \#(O/\psi(\mathrm{Ann}_T(\mathrm{Ker}\psi))),$$

则 $\varphi: R \xrightarrow{\simeq} T$ 为同构. □

那么问题便归结为研究 $((\mathrm{Ker}\phi)/(\mathrm{Ker}\phi)^2)$. 照此便导致了对于自守形式 f 的 $\mathrm{Sym}^2 f$ 的 Selmer 群的研究. 从而知上面定理 12.13 的不等式实际上取等号时等价于下面的等式

$$\#(\mathrm{Sym}^2 f\text{的 Selmer 群}) = (L(2, \mathrm{Sym}^2 f)\text{的代数部分的 } p \text{ 分量})$$

$((\mathrm{Ker}\phi)/(\mathrm{Ker}\phi)^2$ 对应于上式的左端, 而 $O/\psi(\mathrm{Ann}_T(\mathrm{Ker}\psi))$ 则对应于上式右端. 关于 $L(s, \mathrm{Sym}^2 f)$ 请参看 §9.1(e)). 于是, ζ 函数 (L 函数)再次出现了, 并起着重要的作用. 在这样一些重要的情形中 ζ 函数总是出现这件事, 实在是不可思议. 关于上面的 Selmer 群的等式, 如果说在理想类群的情形的话, 则是等式

$$\# A_{\mathbb{Q}(\mu_p)}^{\omega^i} = \#(\mathbb{Z}_p / L(0, \omega^{-i}))$$

(i 为满足 $1 < i < p-1$ 的奇数, §10.3(c) 定理 10.37). 如果这样考虑的话, 那么则可想到问题的公式应是岩泽理论处理的事 (事实上, Wiles 曾这样考虑过).

还有, 岩泽主猜想的证明的方针是通过自守形式构造出所有的非分歧扩域, 而在这里, 遵循的也是通过自守形式构造出所有满足条件的表示这样类似的方针. 为了证明岩泽猜想, 必须要有到 GL_2 的表示以便构造 Abel 扩域. 总之, 如果用 §9.4(b) 的话来说, 就是从 2 阶来观察 1 阶是必要的. 而在这里, 为了研究 2 维表示, 从 $\mathrm{Sym}^2 f$ 这个 3 阶去观察 2 阶也是必要的.

而关于 Selmer 群的不等式的证明在这里不可能叙述了. 最终 Wiles 证明了如果 T 为完全交叉则此不等式成立. 所谓完全交叉是一个关于局部环奇点的信息, 表明奇点的情形不是那么坏. 这最后的难关是由与 R.Taylor 合作的文章克服的.

定理 12.14 (Taylor, Wiles) *T 是完全交叉的.* □

证明是巧妙地使用了 $Nl_1 \cdot \cdots \cdot l_r$ 级的自守形式的 Hecke 环而完成的, 想要进一步详细了解的读者请参看岩波讲座 “现代数学进展” 的《Fermat 猜想》这一卷.

小结

12.1 定义在有理数域上的椭圆曲线的算术中, 在对有限域上的有理点个数的考察中, 在对 Tate 模的作用的考察中, 还有像在对 ζ 函数的考察中都会遇到整数数列 $(a_l)_{l\in\mathcal{L}}$. 由这个重要的整数数列 $(a_l)_{l\in\mathcal{L}}$ 能给出自守形式, 这便是所谓的谷山–志村–Weil 猜想.

12.2 Wiles 对于有理数域上的半稳定椭圆曲线证明了谷山–志村–Weil 猜想. 从而, 按照这个事实, 给予了 Fermat 猜想以肯定的答案.

参考书目

数域及代数数论初步

[1] 藤崎源二郎, 森田康夫, 山本芳彦, 向数学进军 (数学讨论班增刊), 日本评论社, 1980.

[2] 岩泽健吉, 代数函数论, 岩波出版社, 1973(修订本).

[3] 岩泽健吉, 局部类域论, 岩波出版社, 1980.

[4] J.-P. Serre, *A course in arithmetic*, GTM 7, Springer-Verlag.

[5] 高木贞治, 初等整数论讲义, 共立出版社, 1973 (第二版).

[6] 高木贞治, 代数的整数论, 岩波出版社, 1982 (第二版).

[7] 山本芳彦, 数论入门, 丛书"现代数学入门", 岩波出版社, 2003.

[8] A. Weil, *Number Theory: An Approach Through History from Hammurapi to Legendre*, Birkhauser, Boston, 1984.

[9] J.W.S. Cassels and A.Fröhlich, *Algebraic number theory*, Academic Press, 1967.

[10] R. Dedekind, *Theory of algebraic integers*, the Press Syndicate of the University of Cambridge, 1996 (English version), First published in French, 1877.

[11] J.-P. Serre, *Local fields*, GTM 67, Springer-Verlag, 1967.

[12] A. Weil, *Basic number theory*, Springer-Verlag, 1967.

在 [4] 中从二次剩余互反律, p 进域, Hilbert 符号出发开始了简洁明快的讲解. 而 [1], [7] 有许多的实例, 是优秀的数论入门书. [5] 则是一本公认的名著. 就学习数域以及函数域而言, 读一下 [2], [3], [6], [9], [11], [12] 是很好的. [10] 是对代数数论的开创做出很大贡献的数学家自己所写的对代数数的解释. 关于历史方面, [8] 是一本有趣的书.

椭圆曲线

[1] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer-Verlag, 1992.

[2] D. Husemöller, *Elliptic curves*, GTM 111, Springer-Verlag, 1987.

[3] N. Koblitz, *Introduction to elliptic curves and modular forms*, GTM 97, Springer-Verlag, 1993 (second edition).

[4] J. H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.

[5] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, 1994.

[6] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Math., Friedr. Vieweg & Sohn,1990 (second edition).

[7] G. Cornell, J.H. Silverman and G. Stevens (ed), *Modular forms and Fermat's last theorem*, Springer-Verlag, 1997.

[1] 是为初学者写的椭圆曲线的入门书. 在《数论 II》中因篇幅关系而未触及的同余数问题与 Birch, Swinnerton-Dyer 猜想之间的关系, 在 [3] 中有详细的讲解. 另外, Mordell-Weil 定理的证明在《数论 II》中也未曾处理. 在这个定理的证明中, 对于数域上的椭圆曲线的点像在 §1.3 那样, 定义的具有好性质的 “高” 起了本质的作用. 对此, 请参看 [2], [4], [6]. [4], [5] 则是标准的好教科书. 而 [7] 中对于自守形式和 Fermat 猜想都有详细的解说.

ζ 函数

[1] A. Weil, *Basic number theory*, Springer, 1967.

[2] J. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, 1967.

[3] S. Lang, *Algebraic number theory*, Addison-Wesley, 1970.

[4] E. C. Tichmarsh, *The theory of the Riemann zeta-function*, Oxford Univ. Press, 1951(2nd ed. 1986).

[5] H. Edwards, *Riemann's zeta function*, Academic Press, 1974.

[6] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, 1968.

[7] 末纲恕一, 解析的整数论, 岩波出版社, 1950.

[8] 高木贞治, 初等整数论讲义, 共立出版社, 1931.

[9] 河田敬义, 数论, 岩波基础数学选书, 1992.

[10] 藤崎源二郎, 森田康夫, 山本芳彦, 向数学进军 (数学讨论班增刊), 日本评论社, 1980.

对于作为 ζ 函数开端的 Riemann ζ 函数, [4], [5] 有详细叙述. 关于素数定理请参看 [2], [3], [5], [6], [7], [8], [9], [10]. 特别在 [6] 中有关于一般素数定理的系统阐

述. 关于利用 ζ 在阿代尔上的积分进行解析延拓的方法请见 [2] 中 Tate 的原始论文 (1950) 或者 [1], [3]. 另外, 在自守形式相关的文献里也有很多 ζ 函数的记述. 也请参看那里的文献. 譬如, 上面的 [6] 推广了 Tate 的方法到 GL_n 上.

类域论

[1] 弥永昌吉编撰, *数论*, 岩波出版社, 1969.

[2] 岩泽键吉, *局部类域论*, 岩波出版社, 1980.

[3] 高木贞治, *代数的整数论*, 岩波出版社, 1982(第二版).

[4] N. Bourbaki, *Éléments de mathématique, Algébre, Chap.*8, Hermann, Paris.

[5] E. Artin and J. Tate, *Class field theory*, Benjamin, 1967.

[6] J.W.S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, 1967.

[7] D. A. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, 1989.

[8] J.-P. Serre, *Local fields*, GTM 67, Springer-Verlag, 1967.

[9] A. Weil, *Basic number theory*, Springer-Verlag, 1967.

关于中心单代数以及 Brauer 群的一般理论只要参照 [4] 就行, 它对此有详细且缜密的记述. 关于局部域的 Brauer 群请参照 [8], 整体域的 Brauer 群参照 [9]. [2], [8] 叙述了局部类域论, 而整体类域论则在 [1], [3], [5], [6], [9] 中叙述. 倘若读 [1], 那么阅读其历史部分就可以了 (其余部分则没有深入进去). [6] 也对历史有很好的解说. [6] 还给出了对类域论的代数证明.《数论 I》的证明与 [9] 相近. [3] 为对类域论做过很大贡献的作者本人的著述, 颇扣人心弦. [7] 则从素数的形状开始直到类域论为止进行了讲解.

自守形式

[1] G. H. Hardy, *Ramanujan*, Cambridge Univ. Press, 1940.

[2] I. M. Gelfand, M. I. Graev and I. I. Pyatetskii-Shapiro, *Representation theory and automorphic functions*, Saunders, 1969 (Reprint: Academic Press, 1990) (原著为俄文, 1966).

[3] A. Ogg, *Modular forms and Dirichlet series*, Benjamin, 1969.

[4] R. P. Langlands, *Problems in the theory of automorphic forms*, LNM **170** (1970) 18-61, Springer.

[5] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, 1971.

[6] R. Godement and H. Jacquet, *Zeta functions of simple algebras*, LNM **260** (1972), Springer.

[7] S. Lang, *Introduction to modular forms*, Springer, 1976.

[8] H. Jacquet and J. Shalika, A nonvanishing theorem for zeta function of GL_n, *Invent. Math.* 38 (1976) 1-16.

[9] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer, 1984.
[10] S. Gelbart, An elementary introduction to the Langlands program, *Bull. Amer. Math. Soc.* **10** (1984) 177-219.
[11] A. W. Knapp, *Elliptic curves*, Princeton Uni. Press, 1992.
[12] D. Bump, *Automorphic forms and representations*, Cambridge Univ. Press, 1997.
[13] T. N. Bailey and A. W. Knapp (ed), *Representation theory and automorphic forms*, Proceedings of Symposia in Pure Mathematics, **61** (1997).
[14] J.-P. Serre, *A course in arithmetic*, GTM 7, Springer-Verlag.
[15] 土井公二, 三宅敏恒, *自守形式与整数论*, 纪伊国屋书店, 1976.
[16] 清水英夫, *自守函数*, 岩波基础数学选书, 1992.

关于 Ramanujan 的发现请参考 [1] 以及 Ramanujan 的全集和手稿集. 对于自守形式, 请看 [3], [5], [7], [9], [11], [12], [14], [15], [16] 以及 ζ 函数文献中的 [10]. 对于自守表示, [2], [6], [12], [13] 有详细解说. 自守表示的 L 函数的零点不存在于 $\mathrm{Re}(s)=1$ 上的论断 (对于素数定理的类比是必要的事实) 在 [8] 中有用 Eisenstein 级数的证明. [2] 给出了表示论的 Selberg 迹公式. 由 Selberg 自己给出的关于 Selberg 迹公式的形式请见 Selberg 的全集. Langlands 猜想在 [4] 中有系统的阐述, 而在 [10], [12], [13] 中也有讲解.

岩泽理论

[1] K. Iwasawa, *Lectures on p-adic L-functions*, Ann. of Math. Studies 74, Princeton Univ. Press, 1972.
[2] L. Washington, *Introduction to cyclotomic fields*, GTM 83, Springer-Verlag, 1982.
[3] S. Lang, *Cyclotomic fields I, II* (combined second edition), GTM 121, Springer-Verlag, 1990.
[4] *Algebraic number theory in honor of K. Iwasawa*, Advanced Studies in Pure Math. 17, Kinokuniya, 1989.

很遗憾, 并没有关于岩泽理论的日文书. 也就是说, 本书是这样的第一本. [1] 叙述的是 p 进 L 函数的构成, 而且是围绕以 p 进类数公式为中心进行叙述的, 还讲述了《数论 II》中没有讲的由 Stickelberger 元出发如何 (按发现者自己那样) 构造 p 进 L 函数. 只有从岩泽理论创立者的著作中可以体验出深刻的东西来. [2] 可算是岩泽理论的全面的教科书. 而其中还加入了各式各样的有趣话题, 还给出了我们在《数论 II》中省略掉的命题 10.20 的证明. 在 [3] 的附录中, K. Rubin 使用了 (分圆单位的) Euler 系给出了岩泽主理想的证明. 想要进一步深入到这个课题的读者可看一下 [4]. 这本书一开始介绍了岩泽的工作并罗列了他的论文. 还有对于理想类群之外的对象进行处理的岩泽理论方面的论文, 并可了解岩泽理论的现状.

问题解答

第十章

问题 1 由命题 10.3(2)(a), D_r 被 2 和 3 除尽. 另外, 由 (2)(b) 也被 4 除尽.

问题 2 设 p 为奇素数. 根据分解 $\mathbb{Z}_p^\times = (\mathbb{Z}/p)^\times \times (1+p\mathbb{Z}_p)$, 记 $a = (a_1, a_2)$. 由定义有 $a = \omega(a_1)a_2 = \omega(a)a_2$. 于是有 $a^{p^n} = \omega(a)a_2^{p^n}$, 并因为对于任意的 $x \in 1+p\mathbb{Z}_p$ 有 $\lim_{n\to\infty} x^{p^n} = 1$, 从而得到结论. 对于 $p=2$ 则按定义进行就可以了.

问题 3 例如, 对于 n 使用数学归纳法就可以了.

问题 4 像上面命题 10.5 的证明那样, 若

$$L_p(s, \omega^{r_0}) = \sum_{i=0}^{\infty} a_i(s-1+r_0)^i$$

并将其展成幂级数, 则按照命题 10.8 对于所有 $i \geqslant 2$, a_i 被 p^2 除尽. 另外, 因 p 整除 A_1, 有 p^2 整除 a_1. 于是像命题 10.5 的证明那样, 同样得到了结论.

问题 5 使 γ' 对应于 $1+T$, 于是按照它将 $\mathbb{Z}_p[[\mathrm{Gal}\,(K_\infty/K_N)]]$ 与 $\mathbb{Z}_p[[T]]$ 视为等同. 当 Y 具有前者的结构时, 对于 $n \geqslant 1$ 则有

$$\begin{aligned}Y/(1+\gamma'+\cdots+(\gamma')^{p^n-1})Y &\simeq \mathbb{Z}_p[[T]]/(T-p, ((1+T)^{p^n}-1)/T)\\ &\simeq \mathbb{Z}_p/(2p^n).\end{aligned}$$

于是, 根据引理 10.30, 对于 $n > N$ 有

$$\#A_{K_n} = \#(X/Y) + \#(\mathbb{Z}_p/(2p^{n-N})).$$

因此, 岩泽公式成立. (特别地, 有 $\mu = 0, \lambda = 1$.)

现设 Y 具有后者的结构. 当 p 为奇素数时对于 $n \geqslant 1$, 而当 $p = 2$ 时对于 $n \geqslant 2$, 有

$$Y/(1+\gamma'+\cdots+(\gamma')^{p^n-1})Y \simeq \mathbb{Z}_p[[T]]/(T^2-p,((1+T)^{p^n}-1)/T)$$
$$\simeq \mathbb{Z}_p[\sqrt{p}]/(p^n).$$

因此, 至少对于 $n > N+1$ 有

$$\#A_{K_n} = \#(X/Y) + p^{2(n-N)},$$

从而岩泽公式成立. (特别地, 有 $\mu = 0, \lambda = 2$.)

问题 6 (1) 倘若有 $\lambda(G_{\omega^{1-i}}(T)) > 1$, 则由问题 4 有 $\zeta(1+i-p) \equiv \zeta(2+i-2p) (\mathrm{mod}\ p^2)$.

(2) 使用 §10.1(a) 的值便能弄清楚.

(3) 略.

问题 7 由于在 $\mathbb{Z}/p^n(r)$ 上 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ 以 $\kappa(\sigma)^r$ 倍作用, 并考虑到 $\#(\mathbb{Z}/p^n)^\times = (p-1)p^{n-1}$, 则由

$$\#\mathbb{Z}/p^n(r)^{\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})} = p^n \Longleftrightarrow (p-1)p^{n-1}|r.$$

从而得出结论.

第十二章

问题 1 设 l 为奇素数, 并将 $E: y^2 = x^3 - x$ 看为 $\mathbb{F}_l$ 上的椭圆曲线, 那么 E 具有 4 个 2 等分点. 因此, $E(\mathbb{F}_l)$ 具有 4 阶子群, 故其阶数为 4 的倍数.

习题解答

第九章

9.1 (1), (2), (3) 分别通过比较 $E_4^2 = E_8$, $E_4E_6 = E_{10}$, $1728\Delta = E_4E_8 - E_6^2$ 的 Fourier 系数而得到. 譬如, $E_4E_6 = E_{10}$ 可写为

$$\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right) = 1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n,$$

比较两端 q^n 的系数得到

$$240\sigma_3(n) - 504\sigma_5(n) - 240\cdot 504\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m) = -264\sigma_9(n).$$

以 24 除它就得到 (2).

9.2 答案是 $\dfrac{B_k}{2k}$ (B_k 为 Bernoulli 数). 这是在权 k 的 (正则) Eisenstein 级数 $E_k(z)$ 的变换公式 $E_k(-\frac{1}{z}) = z^k E_k(z)$ 中, 当令 $z = i$ 时由 $E_k(i) = i^k E_k(i) = -E_k(i)$ 知 $E_k(i) = 0$, 于是使用

$$E_k(i) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)e^{-2\pi n} = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\frac{n^{k-1}}{e^{2\pi n}-1}$$

便知有此结果.

9.3 (1) 定理 9.16(3) 的式子是

$$e^{-2\pi}\prod_{n=1}^{\infty}(1-e^{-2\pi n})^{24} = \left(\frac{\varpi}{\sqrt{2}\pi}\right)^{12},$$

若对此式取对数便得到了 (1) 的式子.

(2),(3) 使用 Hurwitz 的方法 (定理 9.16 的补充 2) 即可, 也可直接地求出

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m+ni)^8} = 2\zeta(8)E_8(i) = 2\zeta(8)E_4(i)^2$$
$$= 2\left(\frac{\pi^8}{9450}\right)\cdot 9\left(\frac{\varpi}{\pi}\right)^8 = \frac{\varpi^8}{525}$$

以及

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m+ni)^{12}} = 2\zeta(12)E_{12}(i)$$
$$= 2\left(\frac{2^{10}}{13!}\frac{691}{105}\pi^{12}\right)\left(\frac{2^6\cdot 3^5\cdot 7^2}{691}\frac{\varpi^{12}}{2^6\pi^{12}}\right) = \frac{2\varpi^{12}}{53625}.$$

然而, 在 §9.1(b) 的式子

$$E_{12} - E_6^2 = \frac{2^6\cdot 3^5\cdot 7^2}{691}\Delta$$

中代入 $z = i$ 则可求出 $E_{12}(i)$ ($\Delta(i)$ 为定理 9.16(3)).

9.4 (1) 因为 $\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}\in SL_2(\mathbb{Z})$, 故有

$$E_k\left(\frac{-1}{z+1}\right) = (z+1)^k E_k(z).$$

若在此代入 $z=\rho$, 则因 $\dfrac{-1}{\rho+1} = \rho$, $\rho + 1 = -\rho^2$, 故有

$$E_k(\rho) = \rho^{2k}E_k(\rho).$$

因此, 当 $3\nmid k$ 时有 $E_k(\rho) = 0$, 特别地 $E_4(\rho) = 0$.

于是, 若在 $\Delta = \dfrac{E_4^3 - E_6^2}{1728}$ 中设 $z = \rho$, 则

$$E_6(\rho)^2 = -1728\Delta(\rho) = 1728e^{-\sqrt{3}\pi}\prod_{n=1}^{\infty}(1-(-1)^n e^{-\sqrt{3}\pi n})^{24}$$

为正, 从而 $E_6(\rho)\neq 0$.

(2) 因为

$$E_k(\rho) = 1 + \frac{2k}{B_k}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}n^{k-1}}{e^{\sqrt{3}\pi n} + (-1)^{n-1}},$$

那么当 $3\nmid k$ 时因 $E_k(\rho) = 0$ 故有

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}n^{k-1}}{e^{\sqrt{3}\pi n} + (-1)^{n-1}} = -\frac{B_k}{2k}.$$

$k=4, 8$ 已包括在这里了. 在 $k=2$ 时的变换公式 (参看 §9.5(e))

$$E_2\left(\frac{-1}{z+1}\right)=(z+1)^2E_2(z)+\frac{6(z+1)}{\pi i}$$

中以 $z=\rho$ 代入求解, 知有

$$E_2(\rho)=\frac{2\sqrt{3}}{\pi}.$$

因此,

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}n^{k-1}}{e^{\sqrt{3}\pi n}+(-1)^{n-1}}=\frac{\sqrt{3}}{12\pi}-\frac{1}{24}.$$

9.5 (i)⇔(ii) 显然. 来讨论 (ii)⇒(iii), (iii)⇒(iv), (iv)⇒(i).

对于 (ii)⇒(iii), 因为从渐进式有

$$\tau(p^l)=p^{\frac{11}{2}}\frac{\sin(l+1)\theta_p}{\sin\theta_p},$$

故得知

$$|\tau(p^l)|\leqslant p^{\frac{11}{2}l}(l+1).$$

因此, 当 $n=\prod_p p^{l(p)}$ 时有

$$|\tau(n)|=\prod_p|\tau(p^{l(p)})|\leqslant\prod_p p^{\frac{11}{2}l(p)}(l(p)+1)=n^{\frac{11}{2}}d(n).$$

(iii)⇒(iv) 由 $d(n)=O(n^{\varepsilon})$ 得知.

对 (iv)⇒(i) 进行反向证明. 现在设有素数 p 使得 $|\tau(p)|>2p^{\frac{11}{2}}$. 于是, 存在实数 α 使得

$$1-\tau(p)u+p^{11}u^2=\left(1-p^{\frac{11}{2}}\alpha u\right)\left(1-p^{\frac{11}{2}}\alpha^{-1}u\right),$$

并取 $|\alpha|>1$. 此时, 设 $\varepsilon=\dfrac{1}{2}\log_p|\alpha|>0$, 于是可知 $\dfrac{\tau(n)}{n^{\frac{11}{2}+\varepsilon}}$ 是无界的. 实际上, 在

$$\frac{\tau(p^l)}{p^{l(\frac{11}{2}+\varepsilon)}}=\frac{1}{p^{l\varepsilon}}\cdot\frac{\alpha^{l+1}-\alpha^{-(l+1)}}{\alpha-\alpha^{-1}}$$

中, 由于 $\left|\dfrac{\alpha}{p^{\varepsilon}}\right|=\sqrt{|\alpha|}>1$ 故当 $l\to\infty$ 时 $\dfrac{\tau(p^l)}{p^{l(\frac{11}{2}+\varepsilon)}}$ 无界.

9.6 设 K 的实素点个数为 r_1, 复素点个数为 r_2, 于是 $\zeta_K(s)$ 在 $s=0$ 的 Taylor 展开为

$$\zeta_K(s)=-\frac{Rh}{w}s^{r_1+r_2-1}+\cdots$$

(第七章的定理 7.10(4)). 因此可分为三种不同的情形.

(i) $r_1+r_2=1$: $(r_1,r_2)=(1,0),(0,1)$ (有理数域或虚二次域)

(ii) $r_1+r_2=2$: $(r_1,r_2)=(2,0),(1,1),(0,2)$ (实二次域, $\mathbb{Q}(\sqrt[3]{2})$ 这样的三次域, $\mathbb{Q}(\zeta_5)$ 这样的四次域)

(iii) $r_1+r_2\geqslant 3$: 其他.

首先在 (iii) 时有 $\zeta_K'(0)=0$, 且 $\prod\limits_{a} N(a)=1$.

在 (i) 时, 如果 $K=\mathbb{Q}$, 则由定理 9.13 有

$$\zeta_K'(0)=-\frac{1}{2}\log(2\pi),$$

且

$$\prod_{a} N(a)=\prod_{n=1}^{\infty} n=\sqrt{2\pi}.$$

如果 $K=\mathbb{Q}(\sqrt{-1})$, 由定理 9.16(2) 有

$$\zeta_{\mathbb{Q}(\sqrt{-1})}'(0)=-\frac{1}{4}\log\left(\frac{\Gamma\left(\frac{1}{4}\right)^4}{4\pi}\right),$$

且

$$\prod_{a} N(a)=\left(\prod_{m,n=-\infty}^{\infty}{}' (m^2+n^2)\right)^{\frac{1}{4}}=2^{-\frac{1}{2}}\pi^{-\frac{1}{4}}\Gamma\left(\frac{1}{4}\right)=2^{\frac{1}{4}}\varpi^{\frac{1}{2}}.$$

对一般虚二次域也可施行同样的方法 (Lerch(1897年), Chowla–Selberg (1949/1864年) 的结果).

在 (ii) 的情形, 其单位群的阶为 1, 利用 (基本) 单位 ε ($|\varepsilon|>1$) 可记 $R=\log|\varepsilon|$. 于是有

$$\zeta_K'(0)=-\frac{h}{w}\log|\varepsilon|.$$

因此求出

$$\prod_{a} N(a)=|\varepsilon|^{\frac{h}{w}}.$$

这是个代数整数.

第十章

10.1 因为 $\zeta(-1),\cdots,\zeta(-9)$ 的分子不被 p 除尽, 故根据推论 10.38 有

$$A_{\mathbb{Q}(\mu_p)}^{\omega^{p-2}}=\cdots=A_{\mathbb{Q}(\mu_p)}^{\omega^{p-10}}=0.$$

于是, 根据定理 10.36(1) 有

$$X^{\omega^{p-2}}=\cdots=X^{\omega^{p-10}}=0.$$

10.2 (1) 取 $r>2$ 即可. 当展开 $L_p(s,\omega^r)=\sum_{i=0}^{\infty}a_i(s-1+r)^i$ 为幂级数时, 有

$$\zeta(1-r)\equiv L_p(1-r,\omega^r)=a_0\,(\mathrm{mod}\ p^2),$$

并由命题 10.8 知对于所有的 $i\geqslant 2$, a_i 被 p^2 除尽, 故有

$$\zeta(2-r-p)\equiv L_p(2-r-p,\omega^r)\equiv a_0+a_1(1-p)\,(\mathrm{mod}\ p^2).$$

因此有

$$a_1\equiv(\zeta(2-r-p)-\zeta(1-r))/(1-p)\,(\mathrm{mod}\ p^2),$$

从而得知

$$\begin{aligned}L_p(0,\omega^r)&\equiv a_0+a_1(r-1)\\&\equiv((2-r-p)\zeta(1-r)-(1-r)\zeta(2-r-p))/(1-p)\not\equiv 0\,(\mathrm{mod}\ p^2).\end{aligned}$$

因此, 有 $\mathrm{ord}_p(L(0,\omega^{r-1}))=\mathrm{ord}_p(L_p(0,\omega^r))=1$, 再由定理 10.37 得到结论.

(2) 使用 §10.1(a) 的值就清楚了.

10.3 (1) 由岩泽主猜想知 X^{ω^i} 为秩 1 的自由 $\mathbb{Z}_p$ 模. 因此, X^{ω^i} 由单个元在 $\Lambda=\mathbb{Z}_p[[\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p))]]\simeq\mathbb{Z}_p[[T]]$ 上生成. 记 $X^{\omega^i}\simeq\Lambda/(G_{\omega^{1-i}}(T))$. 如果注意到由相伴多项式的定义有 $\mathrm{ord}_p(\alpha)>0$, 则根据定理 10.36, 像问题 5 那样便得到了结论.

(2) 由岩泽主猜想知 X^{ω^i} 为秩 2 的自由 $\mathbb{Z}_p$ 模.

(i) 当 X^{ω^i} 在 Λ 上由一个元生成时. 此时因为

$$X^{\omega^i}\simeq\Lambda/(G_{\omega^{1-i}}(T))\simeq\Lambda/((T-\alpha)(T-\beta)),$$

由定理 10.36 并令 $K_n=\mathbb{Q}(\mu_{p^n})$, 那么对于 $n\geqslant 1$ 便有

$$A_{K_n}^{\omega^i}\simeq\Lambda/((T-\alpha)(T-\beta),(1+T)^{p^{n-1}}-1).$$

在这里若使用 $\mathrm{ord}_p(\alpha)<\mathrm{ord}_p(\beta)$, 则可计算出

$$A_{K_n}\simeq\mathbb{Z}_p/(\alpha\beta p^{n-1})\oplus\mathbb{Z}_p/(p^{n-1}).$$

(ii) 当 X^{ω^i} 在 Λ 上不是由一个元生成时. 此时, X^{ω^i} 在 Λ 上由两个元生成. 取 Λ 模的正合序列

$$0\to\Lambda^2\xrightarrow{f}\Lambda^2\to X^{\omega^i}\to 0,$$

并以 A 表示 f 所对应的矩阵. 若使用 $\mathrm{ord}_p(\alpha-\beta)=1,\mathrm{ord}_p(\alpha)<\mathrm{ord}_p(\beta)$, 则使用初等变换可将 A 变为 $\begin{pmatrix}T-\alpha&0\\0&T-\beta\end{pmatrix}$. 因此, 我们有

$$X^{\omega^i}\simeq\Lambda/(T-\alpha)\oplus\Lambda/(T-\beta),$$

从而

$$A_{K_n} \simeq \mathbb{Z}_p/(\alpha p^{n-1}) \oplus \mathbb{Z}_p/(\beta p^{n-1}).$$

10.4 (1) 对于为单射, 以命题 10.33 同样的方法证明. 至于满射的证明, 当记在 K_n/F_n 为分歧的 F_n 的素理想的集合为 S 时, 使用

$$\left(\bigoplus_{v\in S}\mathbb{Z}_p v)^{\chi}\right) = \left(\bigoplus_{v\in S}\mathbb{Z}_p v\right)\bigotimes_{\mathbb{Z}_p[\mathrm{Gal}\,(F/\mathbb{Q})]} O_{\chi} = 0$$

即可.

(2) 与定理 10.37 大体一样地进行证明.

索　　引

A

B

C

D

E

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z